```
File 348:EUROPEAN PATENTS 1978-2003/Apr W04
         (c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20030501,UT=20030424
         (c) 2003 WIPO/Univentio
? ds

Set     Items   Description
S1     162856   INTRUS????? ? OR INTRUD???? ? OR ATTACK???? ? OR PSEUDOATT-
             ACK? OR VULNERAB? OR HACK???? ? OR CRACK???? ? OR MALICIOUS OR
              UNAUTHORIZ? OR UNAUTHORIS? OR INFILTRAT? OR THREAT?
S2      48953   SECURITY
S3      21062   IDS
S4     131021   PENETRAT? OR BREACH?
S5      13501   S1:S4(3N)(TRACK? OR DETECT? OR MONITOR? OR DISCERN? OR GAU-
             G??? ? OR EXPOS???? ? OR CHECK??? ? OR CHEQU??? ? OR DIAGNOS?-
             ?? ?)
S6       3345   S1:S4(3N)(SELFTEST? OR SELFDIAGNOS? OR DX OR PROBE? ? OR P-
             ROBING? OR ANALYS? OR ANALYZ? OR ANALYT? OR ASSESS????? ? OR -
             BIST)
S7       4925   S1:S4(3N)(EVALUAT? OR SENS?R? ? OR SENSING OR SENSE? ? OR -
             SCREEN?)
S8       1521   NOC OR NETWORK? ?(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CEN-
             TER? ? OR CENTRE? ?)
S9      61370   SOC OR SECURITY(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CENTE-
             R? ? OR CENTRE? ?)
S10    995252   SYSTEM? ?
S11     52503   S10(3N)(INTEGRATED OR MASTER OR PRINCIPAL OR MAIN OR PARENT
              OR HIERARCH? OR TOPOLOG? OR PRIMARY)
S12     24891   SUBSYSTEM? OR SUB()SYSTEM?
S13      3343   S10(3N)(MULTI()(LAYER? OR LEVEL? OR TIER? OR STACK? OR BRA-
             NCH?) OR MULTILAYER? OR MULTILEVEL? OR MULTITIER? OR MULTISTA-
             CK? OR MULTIBRANCH?)
S14      1758   S10(3N)(MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIP-
             LE OR MULTIPLICIT? OR MULTITUD? OR ADDITIONAL)(1W)(LAYER? OR -
             LEVEL? OR TIER? OR STACK? OR BRANCH?)
S15     36821   FIREWALL? OR FIRE()WALL? ? OR ROUTER? ? OR S3
S16        23   MULTIDEVICE?
S17     50927   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
             ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
             VARIOUS OR VARIETY)(1W)DEVICE?
S18      1178   OUTSOURC? OR OUT()SOURC??? ?
S19        91   S5:S7(S)S8:S9
S20       702   S5:S7(S)(S11:S14 OR SUBCOMPONENT? OR SUBMODULE? OR S10(3N)-
            (COMPONENT? OR MODULE?))
S21    107993   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
             ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
             VARIOUS OR VARIETY)(1W)(COMPONENT? OR MODULE?)
S22       125   S19:S20(25N)(S15:S18 OR S21)
S23        53   S19:S20(25N)(S16:S18 OR S21)
S24        19   S5:S7(20N)S8:S9
S25       369   S5:S7(20N)(S11:S14 OR SUBCOMPONENT? OR SUBMODULE? OR S10(3-
            N)(COMPONENT? OR MODULE?))
S26        60   S24:S25(S)(S15:S18 OR S21)
S27        24   S24:S25(S)(S16:S18 OR S21)
S28      9647   IC='G06F-013'
S29      8033   IC='G06F-011'
S30      5085   IC='H04L-009'
S31         7   S23 AND S28:S30
S32        31   S27 OR S31
S33        31   IDPAT (sorted in duplicate/non-duplicate order)
```

S34 31 IDPAT (primary/non-duplicate records only)

34/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00673024
Intrusion detector.
Intrusionsmelder.
Detecteur d'intrusion.
PATENT ASSIGNEE:
STATE OF ISRAEL - MINISTRY OF DEFENCE, (559346), Armament Development Authority, Rafael, P.O.B. 2250, Haifa 31021, (IL), (applicant designated states: DE;FR;GB)
INVENTOR:
Yahav, Giora, 11 Beilis Street, Haifa 34814, (IL)
LEGAL REPRESENTATIVE:
Price, Paul Anthony King (59911), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 645644 A1 950329 (Basic)
APPLICATION (CC, No, Date): EP 94305859 940808;
PRIORITY (CC, No, Date): IL 10661793 930808
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: G01S-017/02;

ABSTRACT EP 645644 A1
A security device for protecting a protected area (110) comprises two laser reflectometer detectors (100). Each detector (100) produces an area swept laser beam (102) aligned to sweep an area outside the protected area and has a time-of-flight detector for detecting reflections by objects in the path of the laser beam outside the protected area. (see image in original document)
ABSTRACT WORD COUNT: 62

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	950329	A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	951025	A1	Date of filing of request for examination: 950830
Withdrawal:	970416	A1	Date on which the European patent application was withdrawn: 970217

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	328
SPEC A	(English)	EPAB95	1545
Total word count - document A			1873
Total word count - document B			0
Total word count - documents A + B			1873

...SPECIFICATION fixed and moving objects, is displayed to an operator.
Thus, the present invention provides comprehensive **intrusion detection** in the vicinity of a protected zone and accomplishes the task using only a minimum **number** of **components** . The **system** is particularly adept for protecting soldiers' quarters in the field, since it is easy to...

34/5,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00541437

In-band/out-of-band alert delivery system
Im-Band/Ausserband-Warnabgabessystem
Systeme de diffusion d'avertissement en bande et hors bande

PATENT ASSIGNEE:
Compaq Computer Corporation, (687792), 20555 S.H. 249, Houston Texas 77070, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;NL;SE)
INVENTOR:
Danielson, Lih-Juan, 16301, Willowpark Drive, Tomball, Texas 77375, (US)
Dobyns, Patrick E., 1726 Parkhurst, Garland, Texas 75040, (US)
Hernandez, Thomas J., 10707 Idlebrook Drive, Houston, Texas 77070, (US)
Neyland, Ronald A., 9131 Herts, Spring, Texas 77379, (US)
Stupek, Richard A., 13555 Breton Rudge, No 1121, Houston, Texas 77070, (US)
Miller, Andrew J., 8450 Willow Place North No. 1604, Houston, Texas 77070 , (US)
Barron, James E., 8902 Sunny Point Drive, Spring, Texas 77379, (US)
Chen, Cheryl X., 16318 Willowpark Drive, Tomball, Texas 77375, (US)
LEGAL REPRESENTATIVE:
Brunner, Michael John (28871), GILL JENNINGS & EVERY Broadgate House 7 Eldon Street, London EC2M 7LH, (GB)
PATENT (CC, No, Kind, Date): EP 520770 A2 921230 (Basic)
EP 520770 A3 931118
EP 520770 B1 971015
APPLICATION (CC, No, Date): EP 92305802 920624;
PRIORITY (CC, No, Date): US 720258 910624
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: G06F-011/30; H04L-012/26;
CITED PATENTS (EP A): EP 4298860 A; WO 8806822 A; WO 8301851 A; US 5603523 A

ABSTRACT EP 520770 A2

An in-band/out-of-band alert delivery system for a computer system manager includes an alert log which maintains a record of alerts to be delivered and the status of those alerts, an alert manager for making a first attempt to deliver each alert, and a retry manager for making subsequent attempts to deliver alerts as becomes necessary and appropriate. The alert delivery system may also include a bus master interface manager for making in-band alert deliveries and a communications manager for making out-of-band alert deliveries. Telephone numbers are provided to the communications manager by an alert destination list. Out-of-band alert deliveries may be made via a modem, a universal asynchronous receiver transmitter, or the like. (see image in original document)
ABSTRACT WORD COUNT: 120

LEGAL STATUS (Type, Pub Date, Kind, Text):
Lapse: 020619 B1 Date of lapse of European Patent in a contracting state (Country, date): AT 19971015, BE 19971015, CH 19971015, LI 19971015, DK 19971015, ES 19971015, GR 19971015, IT 19971015, SE 19980115,
Lapse: 20000202 B1 Date of lapse of European Patent in a contracting state (Country, date): AT 19971015, BE 19971015, CH 19971015, LI 19971015, DK 19971015, GR 19971015, IT 19971015, SE 19980115,
Lapse: 030212 B1 Date of lapse of European Patent in a contracting state (Country, date): AT 19971015, BE 19971015, CH 19971015, LI 19971015, DK 19971015, ES 19971015, GR

19971015, IT 19971015, NL 19971015, SE
19980115,

Application:	921230	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	931118	A3	Separate publication of the European or International search report
Change:	931118	A2	Obligatory supplementary classification (change)
Examination:	940713	A2	Date of filing of request for examination: 940510
Examination:	970129	A2	Date of despatch of first examination report: 961212
Grant:	971015	B1	Granted patent
Lapse:	980520	B1	Date of lapse of the European patent in a Contracting State: SE 980115
Lapse:	980722	B1	Date of lapse of the European patent in a Contracting State: AT 971015, DK 971015, SE 980115
Lapse:	980722	B1	Date of lapse of the European patent in a Contracting State: AT 971015, DK 971015, SE 980115
Oppn None:	981007	B1	No opposition filed
Lapse:	981021	B1	Date of lapse of the European patent in a Contracting State: AT 971015, CH 971015, LI 971015, DK 971015, SE 980115
Lapse:	981021	B1	Date of lapse of the European patent in a Contracting State: AT 971015, CH 971015, LI 971015, DK 971015, SE 980115
Lapse:	981111	B1	Date of lapse of the European patent in a Contracting State: AT 971015, BE 971015, CH 971015, LI 971015, DK 971015, SE 980115
Lapse:	991020	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19971015, BE 19971015, CH 19971015, LI 19971015, DK 19971015, IT 19971015, SE 19980115,

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9710W2	480
CLAIMS B	(German)	9710W2	569
CLAIMS B	(French)	9710W2	616
SPEC B	(English)	9710W2	7053
Total word count - document A			0
Total word count - document B			8718
Total word count - documents A + B			8718

...SPECIFICATION of related art section above, so as to provide enhanced hardware management capabilities. Because these **various components** are discussed in detail in other of the related cases referenced above, they will not...

...to the modem or asynchronous interface of the system manager can be made to require **security checks** before access is allowed. The final **component** of the management **system** listed above, configuration support, involves configuring the 32-Bit intelligent Bus Master EISA board into...

34/5,K/7 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00952969 **Image available**
UNIVERSAL, CUSTOMIZABLE SECURITY SYSTEM FOR COMPUTERS AND OTHER DEVICES
SYSTEME DE SECURITE PERSONNALISABLE, UNIVERSEL, POUR ORDINATEURS ET AUTRES DISPOSITIFS

Patent Applicant/Assignee:
CAVEO TECHNOLOGY LLC, 411 Massachusetts Avenue, Cambridge, MA 02139-4102, US, US (Residence), US (Nationality)
Inventor(s):
EVANS Thomas P, 23 Palmer Street, Watertown, MA 02472-2757, US,
LEE David W, 343 Otis Street, West Newton, MA 02465-2533, US,
GREENWALD Gail C, 23 Myopia Road, Winchester, MA 01890-3713, US,
VERPLAETSE Christopher, 35 Skehan Street, Somerville, MA 02143-3737, US,
Legal Representative:
COLEMAN Roy J (et al) (agent), Iandiorio & Teska, 260 Bear Hill Road, Waltham, MA 02451-1018, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200287152 A1 20021031 (WO 0287152)
Application: WO 2002US11955 20020417 (PCT/WO US0211955)
Priority Application: US 2001284536 20010418
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/32**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6457

English Abstract
A universal, customizable computer security system (50) including a set of security input signals (52) each relating to a possible security event and a rules engine (72) with a universal software interface (74) responsive to the security input signals (54-70). The rules engine (72) is configurable to perform one or more security actions (76-92) in response to each security input signal (54-70). The rules engine (72) further includes a user interface program (94) to allow a user to select one or more customized security actions for a combination of one or more chosen security input signals (54-70) and a universal software output interface (75) responsive to the selected security actions (76-92).

French Abstract
L'invention concerne un systeme de securite informatique personnalisable (50), universel, faisant intervenir une serie de signaux d'entree (52) de securite se rapportant chacun a un evenement de securite possible et un moteur de regles (72) avec une interface logicielle universelle (74) sensible aux signaux d'entree (54-70) de securite. Le moteur de regles (72) peut etre configure pour effectuer une ou plusieurs actions de securite (76-92) en reponse a chaque signal d'entree (54-70) de securite. Le moteur de regles (72) comprend egalement un programme d'interface utilisateur (94) permettant a un utilisateur de selectionner une ou

plusieurs actions de securite personnalisees pour une combinaison d'un ou plusieurs signaux d'entree (54-70) de securite choisis et une interface de sortie logicielle universelle (75) sensible aux actions de securite (76-92) selectionnees.

Legal Status (Type, Date, Text)
Publication 20021031 A1 With international search report.
Publication 20021031 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Main International Patent Class: **H04L-009/32**
Fulltext Availability:
Detailed Description

Detailed Description
... rules. Rules engine 72 is in essence a "language" which allows querying the state of **various components** registered to security **system** 50 and reacts to the status in a way defined by the user or the ...

34/5,K/8 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00949160
SYSTEM AND METHOD FOR MANAGING A DEVICE NETWORK
SYSTEME ET PROCEDE DE GESTION D'UN RESEAU DE DISPOSITIFS
Patent Applicant/Assignee:
VIGILOS INC, Suite 101, 2030 First Avenue, Seattle, WA 98121, US, US (Residence), US (Nationality)
Inventor(s):
ALEXANDER Bruce, 13630 S. Keyport Road N.E., Poulsbo, WA 98370, US,
Legal Representative:
URIBE Mauricio A (agent), Christensen O'Connor Johnson & Kindness PLLC, 1420 Fifth Avenue, Suite 2800, Seattle, WA 98101, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200282301 A1 20021017 (WO 0282301)
Application: WO 2002US10756 20020403 (PCT/WO US0210756)
Priority Application: US 2001281254 20010403
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-015/173
International Patent Class: G06F-015/16
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10849

English Abstract
A system and method for managing a distributed data processing network are provided. A distributed network environment is configured such that

monitoring and control devices are associated with device servers in a secure subnet. Each device server connects with a premises server. According to the present invention, a client computing device utilizing a WWW browser employs a communication protocol to pass commands to device servers and devices through the premises server. In another aspect of the present invention, a distributed computing environment allows multiple device servers to cumulatively process data collected from cameras, sensors, and other attached devices and provide a common computing platform and user interface.

French Abstract
L'invention concerne un systeme et un procede destines a gerer un reseau de traitement de donnees. Un environnement de reseau reparti est concu de facon que des dispositifs de surveillance et de controle soient associes a des serveurs de dispositifs dans un sous-reseau securise. Chaque serveur de dispositif est connecte a un serveur local. Selon la presente invention, un dispositif de calcul client utilisant un navigateur Web fait intervenir un protocole de communication pour passer des commandes aux serveurs de dispositifs et aux dispositifs par l'intermediaire du serveur local. Dans un autre aspect de la presente invention, un environnement de calcul reparti permet a plusieurs serveurs de dispositifs de traiter de maniere cumulative des donnees recueillies a partir de cameras, de detecteurs et d'autres dispositifs associes, et de fournir une plateforme de calcul commune ainsi qu'une interface utilisateur.

Legal Status (Type, Date, Text)
Publication 20021017 A1 With international search report.
Examination 20030220 Request for preliminary examination prior to end of 19th month from priority date
Fulltext Availability:
Detailed Description

Detailed Description
... of the user. While the system of the present invention is utilized to integrate traditional **security monitoring** functions, it is also utilized to integrate any information input in a like manner.

With reference to FIGURE 2, the **integrated** information **system** 30 includes a premises server 32 that functions as a communication gateway between **various** monitoring **devices** 36 and control devices 38 and the integrated information system 30.

The premises server 32...

34/5,K/9 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00916586 **Image available**
INTEGRATED INTELLIGENT INTER/INTRA-NETWORKING DEVICE
DISPOSITIF INTELLIGENT INTEGRE D'INTER/INTRARESEAUTAGE
Patent Applicant/Assignee:
SOORIYA NETWORKS INC, 600 Meridian Avenue, Suite 100, San Jose, CA 951126 , US, US (Residence), US (Nationality)
Inventor(s):
VAIRAVAN Kannan P, 7625 Westhill Lane, Cupertino, CA 95014, US,
Legal Representative:
NORTH Michael V (et al) (agent), Fenwick & West Llp, Two Palo Alto Square, Palo, Alto CA 94306, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200250680 A1 20020627 (WO 0250680)
Application: WO 2001US50023 20011220 (PCT/WO US0150023)
Priority Application: US 2000258156 20001221; US 2001894224 20010627
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-011/30**
International Patent Class: G06F-012/14; G06F-015/16; G06F-015/173; **H04L-009/00** ; **H04L-009/32**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12566

English Abstract
An integrated, easily upgradeable networking device (110) capable of interfacing with different types of networks (105a, 105b, 105c, 105d) while still providing high performance networking functionalities such as protocol conversion, security maintenance, and inter/intra-network management within an enterprise environment is described. The device (110) may perform various networking functions within an enterprise and is easily adaptable to perform both inter-networking functions as well as intra-networking functions.
French Abstract
L'invention concerne un dispositif de reseautage integre (110) facilement extensible pouvant faire interface avec differents types de reseaux (105a, 105b, 105c, 105d) tout en conservant des fonctionnalites de reseautage a hautes performances, notamment en termes de conversion de protocole, de maintien de securite et de gestion d'interreseau/intrareseau dans un environnement d'entreprise. Ce dispositif (110) peut executer diverses fonctions de reseautage au sein d'une entreprise. Il est facilement adaptable en vue de l'execution de fonctions d'interreseautage ou d'intrareseautage.

Legal Status (Type, Date, Text)
Publication 20020627 A1 With international search report.
Publication 20020627 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Main International Patent Class: **G06F-011/30**
...International Patent Class: **H04L-009/00** ...

... **H04L-009/32**
Fulltext Availability:
Detailed Description

Detailed Description
... components to function properly as well as coordinates and supervises the activities perfonned by the **components** . The **system** processor 215 may upgrade software and tables stored within the **various components** or devices on an attached network. Additionally, the system processor 21 5 may coordinate with...

34/5,K/10 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00912753 **Image available**
SYSTEM AND METHOD FOR IMPLEMENTING OPEN-PROTOCOL REMOTE DEVICE CONTROL
SYSTEME ET PROCEDE PERMETTANT DE METTRE EN OEUVRE UNE COMMANDE DE DISPOSITIF ELOIGNE A PROTOCOLE OUVERT

Patent Applicant/Assignee:
VIGILOS INC, 2030 First Avenue, Suite 101, Seattle, WA 98121, US, US (Residence), US (Nationality)
Inventor(s):
ALEXANDER Bruce, 13630 S. Keyport Road NE, Poulsbo, WA 98370, US,
BAHNEMAN Liem, 15764 -111th Avenue NE, Bothell, WA 98011, US,
Legal Representative:
URIBE Mauricio A (agent), Christensen O'Connor Johnson Kindness PLLC, Suite 2800, 1420 Fifth Avenue, Seattle, WA 98101-2347, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200246901 A1 20020613 (WO 0246901)
Application: WO 2001US47846 20011206 (PCT/WO US0147846)
Priority Application: US 2000254031 20001206
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-003/00
International Patent Class: G06F-017/30; G06F-015/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8214

English Abstract
A system and method for implementing open-protocol remote device control (224) are provided. A user accesses a common user interface for controlling one or more networked devices. Utilizing the interface, the user selects one or more actions. The selection is encoded in a standard protocol and transmitted to a premises server (202). The premises server (202) obtains the selection, accesses a device interface database and translates the selection into a device-specific protocol. The translated instruction is transmitted to the selected device for implementation. The user interface then obtains any device return data for display on the user interface.

French Abstract
L'invention porte sur un systeme et un procede permettant de mettre en oeuvre une commande (224) de dispositif eloigne a protocole ouvert. Un utilisateur accede a une interface utilisateur commune pour commander un ou plusieurs dispositifs en reseau. L'utilisateur selectionne une ou plusieurs actions par l'intermediaire de l'interface. La selection est codee dans un protocole standard, puis transmise a un serveur de locaux (202). Ce serveur de locaux (202) recoit la selection, accede a une base de donnees de l'interface du dispositif et traduit la selection dans un

protocole specifique au dispositif. L'instruction ainsi traduite est transmise au dispositif selectionne pour etre appliquee. L'interface utilisateur recoit ensuite des donnees retour quelconques du dispositif en vue d'un affichage sur l'interface utilisateur.

Legal Status (Type, Date, Text)
Publication 20020613 A1 With international search report.
Publication 20020613 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20030116 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... 238.

Although illustrative embodiments of the present invention have been described with regard to an **integrated** infon-nation **system** 200 configured for **security** **monitoring** , the present invention is not limited to such an implementation. Any networked device capable of...

...network, in which a dedicated device server is utilized,
The present invention facilitates use of **multiple** , dissimilar **devices** by providin
. g
standard interface templates. Additionally, by establishing a dedicated communication channel with the...

34/5,K/12 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00893530 **Image available**
SYSTEM AND METHOD FOR PROVIDING CONFIGURABLE SECURITY MONITORING UTILIZING AN INTEGRATED INFORMATION PORTAL
SYSTEME ET PROCEDE DE SURVEILLANCE DE SECURITE UTILISANT UN PORTAIL INTEGRE D'INFORMATIONS

Patent Applicant/Assignee:
VIGILOS INC, 2030 First Avenue, Suite 101, Seattle, WA 98121, US, US (Residence), US (Nationality)
Inventor(s):
BARKER Geoffrey T, 10034 NE Knight Road, Bainbridge Island, WA 98110, US,

ALEXANDER Bruce, 13630 S. Keyport Road NE, Poulsbo, WA 98370, US,
TALLEY Paul, 20230 NE Novelty Hill Road, Redmond, WA 98053, US,
Legal Representative:
URIBE Mauricio A (agent), Christensen O'Connor Johnson Kindness PLLC, Suite 2800, 1420 Fifth Avenue, Seattle, WA 98101-2347, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200227688 A1 20020404 (WO 0227688)
Application: WO 2001US30326 20010928 (PCT/WO US0130326)
Priority Application: US 2000236282 20000928; US 2001761339 20010116
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G08B-029/00
International Patent Class: G08B-001/08
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9068

English Abstract
A system and method for implementing a configurable security monitor utilizing an integrated information portal. A premises server (32) is in communication with a variety of information sources (34, 36) that produce monitoring data for a defined monitoring target, such as a premises. The premises server (32) transmits the monitoring data to a central server (56) that receives the data and traverses one or more logical rule sets to determine whether the inputted data violates the rules. The rules are generally specified by a user, such as a system administrator to define the level of monitoring desired and an appropriate response in the evaluation of the monitoring data against the rule. Based on an evaluation of the rules, the central server then generates outputs in the form of communication to one or more authorized users via a variety of communication mediums and devices and/or the instigation of a variety of acts.

French Abstract
L'invention porte sur un systeme et un procede de mise en oeuvre d'un surveillant de securite utilisant un portail integre d'informations. Un serveur (32) de locaux, en communication avec diverses sources (34, 36)

d'information produit des donnees de surveillance relatives a une cible a surveiller definie telle qu'un local, et les transmet a un serveur (56) central qui, les recevant, parcourt un ou plusieurs ensembles de regles logiques pour determiner si les donnees entrees violent ou non les regles. Les regles sont generalement indiquees par un utilisateur, par exemple un administrateur du systeme, pour definir le niveau de suivi desire et la reponse appropriee a l'evaluation des donnees de suivi violant la regle. Se basant sur l'evaluation des regles, le serveur central cree alors des donnees de sortie sous la forme de communications a destination d'un ou plusieurs utilisateurs autorises via divers supports et dispositifs de communication et/ou d'instigation de divers actes.

Legal Status (Type, Date, Text)
Publication 20020404 A1 With international search report.
Publication 20020404 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20021121 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... sensors and/or video cameras within the premises.

While the conventional art generally discloses utilizing **multiple** monitoring **devices** to perform various functions, conventional systems are deficient in having a lack of data management functionality and integration. **Security** data from different **monitoring** device types is generally not **integrated** to affect the **system** reporting and -I control. Instead' the conventional security system is built around independent standalone devices...

34/5,K/13 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00893378 **Image available**
SYSTEM AND METHOD FOR PROVIDING CONFIGURABLE SECURITY MONITORING UTILIZING AN INTEGRATED INFORMATION SYSTEM
SYSTEME ET PROCEDE PERMETTANT D'ASSURER UNE SURVEILLANCE DE SECURITE CONFIGURABLE A L'AIDE D'UN SYSTEME D'INFORMATION INTEGRE
Patent Applicant/Assignee:
VIGILOS INC, 2030 First Avenue, Suite 101, Seattle, WA 98121, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
BARKER Geoffrey T, 10034 NE Knight Road, Bainbridge Island, WA 98110, US, US (Residence), US (Nationality), (Designated only for: US)
BAHNEMAN Liem, 15764 - 111th Avenue NE, Bothell, WA 98011, US, US (Residence), US (Nationality), (Designated only for: US)
ANDERSON Claire, 2712 NE 62nd Street, Seattle, WA 98115, US, US (Residence), US (Nationality), (Designated only for: US)
ALEXANDER Bruce, 13630 S. Keyport Road NE, Poulsbo, WA 98370, US, US (Residence), US (Nationality), (Designated only for: US)
TALLEY Paul, 20230 NE Novelty Hill Road, Redmond, WA 98053, US, US (Residence), US (Nationality), (Designated only for: US)
SWENSON Marcus, 6710 Sycamore Avenue NW, Seattle, WA 98117, US, US

(Residence), US (Nationality), (Designated only for: US)
Legal Representative:
URIBE Mauricio A (agent), Christensen O'Connor Johnson Kindness PLLC, Suite 2800, 1420 Fifth Avenue, Seattle, WA 98101-2347, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200227518 A1 20020404 (WO 0227518)
Application: WO 2001US42360 20010928 (PCT/WO US0142360)
Priority Application: US 2000236282 20000928; US 2001281258 20010403; US 2001825506 20010403
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-015/16
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 14233

English Abstract
A system and method for implementing an integrated information system is provided. A premises server (32) is in communication with a variety of information sources that produce monitoring data for a premises. The premises server collects, presents, and transmits the monitoring device data to a central server (56) over the Internet (20). Where the central server is capable of processing data from multiple premises servers. The central server receives the data and traverses one or more logical rule sets to determine whether thw inputted data violates the rules. Based on an evaluation of the rules, the central server generates output in the form of communication to one or more authorized users via a variety of communication mediums and devices and/or the instigation of a variety of acts corresponding to the evaluation of the rules.

French Abstract
L'invention concerne un systeme et un procede concus pour mettre en oeuvre un systeme d'information integre. Un serveur de local (32) est en communication avec diverses sources d'information qui produisent des donnees de surveillance pour un local. Le serveur de local recueille, presente et transmet les donnees du dispositif de surveillance a un serveur central (56) sur l'Internet (20). Ledit serveur central peut traiter des donnees provenant d'une pluralite de serveurs de locaux. Il recoit les donnees et parcourt au moins un ensemble de regles logiques pour determiner si les donnees introduites violent ces regles. Sur la base de l'evaluation des regles, le serveur central produit des sorties sous la forme de communications a destination d'au moins un utilisateur autorise par le biais de divers supports et dispositifs de communication et/ou la demande de diverses actions correspondant a l'evaluation des regles.

Legal Status (Type, Date, Text)
Publication 20020404 A1 With international search report.
Correction 20021024 Corrected version of Pamphlet: pages 1/16-16/16, drawings, replaced by new pages 1/15-15/15; due to late transmittal by the receiving Office
Republication 20021024 A1 With international search report.

Examination 20030206 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description
Detailed Description
... and/or video cameras withi n the premises.

While the conventional art generally discloses utilizing **multiple** monitoring **devices** to perform various functions, conventional systems are deficient in data management functionality and integration. **Security** data from different **monitoring** device types is generally not **integrated** to affect the **system** reporting and control.

Instead, the conventional security system is built around independent stand-alone devices...

34/5,K/14 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00893309 **Image available**
METHOD AND PROCESS FOR CONFIGURING A PREMISES FOR MONITORING
PROCEDE ET TRAITEMENT POUR LA CONFIGURATION DE LOCAUX POUR L'INSTALLATION DE DISPOSITIFS DE CONTROLE
Patent Applicant/Assignee:
VIGILOS INC, 2030 First Avenue, Suite 101, Seattle, WA 98121, US, US (Residence), US (Nationality)
Inventor(s):
ALEXANDER Bruce, 13630 S. Keyport Road NE, Poulsbo, WA 98370, US,
GROSE Karen, 121 Vine Street, #906, Seattle, WA 98121, US,
SCHEBEL Christoph, P.O. Box 1256, Suquamish, WA 98121, US,
ANTAL David, 9674 Topsail Place, Silverdale, WA 98383, US,
Legal Representative:
URIBE Mauricio A (agent), Christensen O'Connor Johnson & Kindness PLLC, Suite 2800, 1420 Fifth Avenue, Seattle, WA 98101-2347, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200227438 A2-A3 20020404 (WO 0227438)
Application: WO 2001US42359 20010928 (PCT/WO US0142359)
Priority Application: US 2000236282 20000928; US 2001281256 20010403
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-015/173
International Patent Class: G06F-015/177
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13409

English Abstract
A system and method for configuring an integrated information system

(200) through a common user interface are provided. A user acces a graphical user interface and selects client, premises, location, monitoring device (206), and processing rule information.The graphical user interface (414) transmits the user selection to a processing server, which configures one or more monitoring devices according to the user selections.

French Abstract

L'invention porte sur un systeme et sur un procede de configuration d'un systeme d'informations integre par l'intermediaire d'une interface utilisateur commune. Un utilisateur accede a une interface graphique et selectionne un client, des locaux, un dispositif de controle et des informations relatives aux regles de traitement. L'interface utilisateur graphique transmet la selection utilisateur a un serveur de traitement qui configure un ou plusieurs dispositifs de controle conformement aux selections utilisateur.

Legal Status (Type, Date, Text)

Publication	20020404	A2 Without international search report and to be republished upon receipt of that report.
Search Rpt	20020627	Late publication of international search report
Republication	20020627	A3 With international search report.
Examination	20021010	Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:

Detailed Description

Detailed Description

... sensors and/or video cameras within the premises.

While the conventional art generally discloses utilizing **multiple** monitoring **devices** to perfon'n various functions, conventional systems are deficient in data management functionality and integration. **Security** data from different **monitoring** device types is generally not **integrated** to affect the **system** reporting and control.

Instead, the conventional security system is built around independent stand-alone devices...

34/5,K/25 (Item 25 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00524844
COMPUTER SECURITY
SECURITE INFORMATIQUE
Patent Applicant/Assignee:
BINDVIEW DEVELOPMENT CORPORATION,
Inventor(s):
SHOSTACK Adam,
ALLOUCH David,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9956196 A1 19991104
Application: WO 99US9622 19990430 (PCT/WO US9909622)
Priority Application: US 9870617 19980430
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: G06F-001/00
International Patent Class: G06F-009/44
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7759

English Abstract
The invention relates to providing enhancements automatically to computer security software whenever the enhancement becomes available. The invention also relates to providing automatically an update to computer security software and integrating the update into the software.

French Abstract
L'invention concerne des ameliorations apportees automatiquement a un logiciel de securite informatique lorsque celles-ci sont disponibles. L'invention concerne egalement une mise a jour automatique d'un logiciel de securite informatique, et l'integration de cette mise a jour dans ledit logiciel.

Fulltext Availability:
Detailed Description

Detailed Description
... application responsible for receiving the software enhancements.

In another aspect, the invention relates to an **integrated system** for **assessing vulnerabilities** . The **integrated system** includes a database of security vulnerabilities and **various modules** . A first module accesses the database and **assesses security vulnerabilities** of an operating system of a computer. A second module accesses the database and assesses...source code.

An Intefzrated Security System
The database of security vulnerabilities is part of an **integrated system** that provides a secure operating environment. The disclosed invention is an **integrated system** for **assessing** computer **security**

vulnerabilities The **integrated system** includes a database of security vulnerabilities and **various modules** . A first module accesses the database and **assesses security vulnerabilities** of an operating system of a computer. A second module accesses the database and assesses ...

34/5,K/26 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2003 WIPO/Univentio. All rts. reserv.

00524843 **Image available**
COMPUTER SECURITY
SECURITE INFORMATIQUE
Patent Applicant/Assignee:
BINDVIEW DEVELOPMENT CORPORATION,
Inventor(s):
SHOSTACK Adam,
ALLOUCH David,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9956195 A1 19991104
Application: WO 99US9454 19990430 (PCT/WO US9909454)
Priority Application: US 9870698 19980430
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: G06F-001/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6594

English Abstract
In one aspect, the invention relates to automatically providing enhancements to computer security software whenever the enhancement becomes available. In another aspect, the invention relates to an integrated system for assessing security vulnerabilities of a computer and/or a computer network.

French Abstract
Un aspect de cette invention concerne l'ajout automatique d'ameliorations a des logiciels de securite informatique chaque fois que l'amelioration devient disponible. Un autre aspect de l'invention concerne un systeme integre qui evalue la vulnerabilite au niveau de la securite d'un ordinateur et/ou d'un systeme informatique.

Fulltext Availability:
Detailed Description

Detailed Description
... source code.

An Integrated Security System
The database of security vulnerabilities is part of an **integrated system** that provides a secure operating environment. The disclosed invention is an **integrated system** for **assessing** computer **security**

vulnerabilities The **integrated system** includes a database of security vulnerabilities and **various modules** . A first module accesses the database and **assesses security vulnerabilities** of an operating system of a computer. A second module accesses the database and assesses ...

```
File 347:JAPIO Oct 1976-2002/Dec(Updated 030402)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200329
         (c) 2003  Thomson Derwent
? ds

Set     Items   Description
S1     261855   INTRUS????? ? OR INTRUD???? ? OR ATTACK???? ? OR PSEUDOATT-
             ACK? OR VULNERAB? OR HACK???? ? OR CRACK???? ? OR MALICIOUS OR
              UNAUTHORIZ? OR UNAUTHORIS? OR INFILTRAT? OR THREAT?
S2      61000   SECURITY
S3       2902   IDS
S4     180079   PENETRAT? OR BREACH?
S5      14829   S1:S4(3N)(TRACK? OR DETECT? OR MONITOR? OR DISCERN? OR GAU-
             G??? ? OR EXPOS???? ? OR CHECK??? ? OR CHEQU??? ? OR DIAGNOS?-
             ?? ?)
S6       1349   S1:S4(3N)(SELFTEST? OR SELFDIAGNOS? OR DX OR PROBE? ? OR P-
             ROBING? OR ANALYS? OR ANALYZ? OR ANALYT? OR ASSESS????? ? OR -
             BIST)
S7       4469   S1:S4(3N)(EVALUAT? OR SENS?R? ? OR SENSING OR SENSE? ? OR -
             SCREEN?)
S8        342   NOC OR NETWORK? ?(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CEN-
             TER? ? OR CENTRE? ?)
S9       1178   SOC OR SECURITY(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CENTE-
             R? ? OR CENTRE? ?)
S10   2707521   SYSTEM? ?
S11     41911   S10(3N)(INTEGRATED OR MASTER OR PRINCIPAL OR MAIN OR PARENT
              OR HIERARCH? OR TOPOLOG? OR PRIMARY)
S12     10790   SUBSYSTEM? OR SUB()SYSTEM?
S13      2104   S10(3N)(MULTI()(LAYER? OR LEVEL? OR TIER? OR STACK? OR BRA-
             NCH?) OR MULTILAYER? OR MULTILEVEL? OR MULTITIER? OR MULTISTA-
             CK? OR MULTIBRANCH?)
S14       453   S10(3N)(MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIP-
             LE OR MULTIPLICIT? OR MULTITUD? OR ADDITIONAL)(1W)(LAYER? OR -
             LEVEL? OR TIER? OR STACK? OR BRANCH?)
S15     11626   FIREWALL? OR FIRE()WALL? ? OR ROUTER? ? OR S3
S16        10   MULTIDEVICE?
S17     21851   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
             ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
             VARIOUS OR VARIETY)(1W)DEVICE?
S18       232   OUTSOURC? OR OUT()SOURC??? ?
S19         0   S5:S7(S)S8:S9
S20       133   S5:S7(S)(S11:S14 OR SUBCOMPONENT? OR SUBMODULE? OR S10(3N)-
             (COMPONENT? OR MODULE?))
S21     60360   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
             ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
             VARIOUS OR VARIETY)(1W)(COMPONENT? OR MODULE?)
S22         1   S5:S7 AND S8:S9
S23       338   S5:S7 AND (S11:S14 OR SUBCOMPONENT? OR SUBMODULE? OR S10(3-
             N)(COMPONENT? OR MODULE?))
S24        30   S22:S23 AND (S15:S18 OR S21)
S25    138543   IC='G06F-013'
S26     10581   IC='G06F-011/30'
S27     24844   IC='H04L-009'
S28        47   S25 AND S26 AND S27
S29         6   S28 AND (S8:S9 OR S11:S14 OR S16:S18 OR S21 OR SUBCOMPONEN-
             T? OR SUBMODULE? OR S10(3N)(COMPONENT? OR MODULE?))
S30         0   S25 AND S26:S27 AND S8:S9
S31       180   S25 AND S26:S27 AND (S11:S14 OR S21 OR SUBCOMPONENT? OR SU-
             BMODULE? OR S10(3N)(COMPONENT? OR MODULE?))
```

```
S32          40   S25 AND S26:S27 AND S16:S18
S33           1   S31 AND S32
S34        5970   MC='T01-H07C5A'
S35        7005   MC='T01-J12C'
S36         505   S34 AND S35
S37           1   S36 AND S8:S9
S38          31   S36 AND (S11:S14 OR S21 OR SUBCOMPONENT? OR SUBMODULE? OR -
                  S10(3N)(COMPONENT? OR MODULE?))
S39           4   S36 AND S16:S18
S40           9   S38 AND S26:S27
S41          19   S22:S23 AND (S16:S18 OR S21)
S42          38   S29 OR S33 OR S37 OR S39:S41
S43          38   IDPAT (sorted in duplicate/non-duplicate order)
S44          38   IDPAT (primary/non-duplicate records only)
```

44/9/4 (Item 4 from file: 350)

014933715 **Image available**
WPI Acc No: 2002-754424/200282
XRPX Acc No: N02-594244

Hierarchical **management** system **implements encryption communication using SPD delivered from management device to VPN devices through relay management units**

Patent Assignee: MITSUBISHI ELECTRIC CORP (MITQ)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2002261829	A	20020913	JP 200151345	A	20010227	200282	B

Priority Applications (No Type Date): JP 200151345 A 20010227
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2002261829	A		17	H04L-012/56	

Abstract (Basic): JP 2002261829 A

NOVELTY - A management device (100) delivers security policy data (SPD) to VPN devices (300-a - 300-y) through relay management units (200-a - 200-n). The encryption communication is established using the SPD.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for hierarchical management method.

USE - **Hierarchical** management **system** .

ADVANTAGE - **Many** VPN **devices** can be managed efficiently and reliably.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of **hierarchical** management **system** . (Drawing includes non-English language text).

Management device (100)
Relay management units (200-a - 200-n)
VPN devices (300-a - 300-y)
pp; 17 DwgNo 1/18

Title Terms: HIERARCHY; MANAGEMENT; SYSTEM; IMPLEMENT; ENCRYPTION; COMMUNICATE; DELIVER; MANAGEMENT; DEVICE; DEVICE; THROUGH; RELAY; MANAGEMENT; UNIT
Derwent Class: W01
International Patent Class (Main): H04L-012/56
International Patent Class (Additional): **G06F-013/00** ; **H04L-009/08** ; H04L-012/22
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05A; W01-A06B7E; W01-A06E; W01-A06G2

44/9/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014753270 **Image available**
WPI Acc No: 2002-573974/200261
XRPX Acc No: N02-454861

Networked device controlling method for security - monitoring **network, involves transmitting selected standard communication protocol instruction to server and obtaining output corresponding to selected networked device**

Patent Assignee: VIGILOS INC (VIGI-N); ALEXANDER B (ALEX-I); BAHNEMAN L (BAHN-I)
Inventor: ALEXANDER B; BAHNEMAN L
Number of Countries: 097 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020068984	A1	20020606	US 2000254031	A	20001206	200261	B
			US 200113408	A	20011206		
WO 200246901	A1	20020613	WO 2001US47846	A	20011206	200261	
AU 200226082	A	20020618	AU 200226082	A	20011206	200262	

Priority Applications (No Type Date): US 2000254031 P 20001206; US 200113408 A 20011206
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020068984	A1		19	G05B-011/01	Provisional application US 2000254031

WO 200246901 A1 E G06F-003/00
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW
AU 200226082 A G06F-003/00 Based on patent WO 200246901

Abstract (Basic): US 20020068984 A1

NOVELTY - A user interface application is obtained corresponding to selected networked device to be manipulated. The operation information corresponding to the selected device is encoded according to a standard communication protocol instruction. The protocol instruction is then transmitted to a server and the output corresponding to the selected device is obtained.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Computer readable recorded medium storing networked device control program;

(2) Computer system; and

(3) Interface providing method.

USE - For controlling networked devices such as **security monitoring** networked devices e.g. smoke, fire, carbon monoxide, window-access, glass break, motion and audio/video detectors, image capture device e.g. video camera, still camera, etc., microphone, finger print, facial, retinal or other biometric identification devices, etc., through common, remote user interface.

ADVANTAGE - Facilitate use of **multiple** , dissimilar **devices** , by providing standard interface templates. Mitigates unnecessary processing steps that impede the flow of communication. Allows increased scalability of the number of monitoring devices used in the

integrated information **system** and controlled by common user interface, by providing dedicated communication channel.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of Internet environment.

pp; 19 DwgNo 1/9

Title Terms: DEVICE; CONTROL; METHOD; SECURE; MONITOR; NETWORK; TRANSMIT; SELECT; STANDARD; COMMUNICATE; PROTOCOL; INSTRUCTION; SERVE; OBTAIN; OUTPUT; CORRESPOND; SELECT; DEVICE

Derwent Class: T01; W01; W05

International Patent Class (Main): G05B-011/01; G06F-003/00

International Patent Class (Additional): G05B-015/00; G05B-023/02; G06F-015/00; G06F-017/30

File Segment: EPI

Manual Codes (EPI/S-X): T01-N01D1B; T01-N01D3; T01-S03; W01-A06B5B; W01-A06F5; W05-D06E; W05-D07C; W05-D08C1

44/9/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014128225 **Image available**
WPI Acc No: 2001-612435/200171
XRPX Acc No: N01-457201

Authentication of hardware and software in networked system **involves central test** module **connected to** system **bus checking authenticity and/or integrity assurance characteristics**

Patent Assignee: SIEMENS AG (SIEI); INFINEON TECHNOLOGIES AG (INFN)
Inventor: EITEL P; RETZOW U; VON DER HEIDT G
Number of Countries: 029 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 1126655	A1	20010822	EP 2000103075	A	20000215	200171 B
WO 200161961	A2	20010823	WO 2001EP1055	A	20010201	200171
EP 1287655	A2	20030305	EP 2001903686	A	20010201	200319
			WO 2001EP1055	A	20010201	

Priority Applications (No Type Date): EP 2000103075 A 20000215
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1126655	A1	G	7	H04L-009/32	
WO 200161961	A2	G		H04L-029/06	
EP 1287655	A2	G		H04L-029/06	Based on patent WO 200161961

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

WO 200161961 A2 G H04L-029/06
Designated States (National): HU JP US
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

EP 1287655 A2 G H04L-029/06 Based on patent WO 200161961
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

Abstract (Basic): EP 1126655 A1

NOVELTY - The method involves **system components** (SK1-SKn) having authentication characteristics (K1-Kn) for hardware modules and/or further authentication or integrity assurance characteristics (S1-Sn) for the software modules. A central test module (PM) connected to the system bus (SB) checks the authenticity characteristics and/or integrity assurance characteristics. An information module (IM) is connected to the test module to output its signals.

USE - For authenticating hardware and software in a networked system.

ADVANTAGE - The hardware/software system is protected against unauthorized manipulation.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic representation of a **system** with **components** connected via a **system** bus

system components (SK1-SKn)
authentication characteristics (K1-Kn)
integrity assurance characteristics (S1-Sn)
information module (IM)
pp; 7 DwgNo 1/1

Title Terms: AUTHENTICITY; HARDWARE; SOFTWARE; SYSTEM; CENTRAL; TEST; MODULE; CONNECT; SYSTEM; BUS; CHECK; AUTHENTICITY; INTEGRITY; ASSURE; CHARACTERISTIC
Derwent Class: S01; S02; T01; W01
International Patent Class (Main): **H04L-009/32** ; H04L-029/06
International Patent Class (Additional): G01R-021/133; G06F-001/00

File Segment: EPI
Manual Codes (EPI/S-X): S01-D02; S01-G04; S01-H07; S02-J02E; T01-G05C;
T01-H01C2; **T01-H07C5A** ; **T01-J12C** ; W01-A05B; W01-A06B1

44/9/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013843494 **Image available**
WPI Acc No: 2001-327707/200134
XRPX Acc No: N01-235769

Apparatus for remotely managed local network interface security providing secure communications between local and wide area networks such as the Internet

Patent Assignee: PERRY G (PERR-I)
Inventor: PERRY G
Number of Countries: 018 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200072171	A1	20001130	WO 2000US14279	A	20000524	200134	B

Priority Applications (No Type Date): US 2000863101 A 20000524; US 99135790 P 19990524
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200072171	A1	E	27	G06F-015/177	

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Abstract (Basic): WO 200072171 A1

NOVELTY - A local area network (LAN) (100) can connect user endpoint devices (102) and includes a telecommunication provider network connection device (104) connected to the Internet or other wide area network (WAN) (106) via a secure universal network appliance (SUNA) (108), performing filtering and encryption operations on transfers. One endpoint device can be connected directly to the SUNA and a **network security operation center** (110) may up-link encryption parameters to the SUNA, while transferring alarms to the connection device. The SUNA can be maintained and operated by trained computer security professionals.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a method of controlling traffic between local and wide area networks.

USE - Remote connection management and monitoring of message traffic between local and remote area networks.

ADVANTAGE - Providing **out - source** management of communication security.

DESCRIPTION OF DRAWING(S) - The drawing is a block diagram of an example system according to the invention

LAN (100)
Endpoint devices (102)
Network connection device (104)
WAN (106)
SUNA (108)
Security operation center (110)
pp; 27 DwgNo 1/5

Title Terms: APPARATUS; REMOTE; LOCAL; NETWORK; INTERFACE; SECURE; SECURE; COMMUNICATE; LOCAL; WIDE; AREA; NETWORK
Derwent Class: T01; W01
International Patent Class (Main): G06F-015/177
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-F05B; **T01-H07C5A** ; T01-H07C5E; **T01-J12C** ; W01-A05A; W01-A06B7; W01-A06E1; W01-A06G3

44/9/14 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013371167 **Image available**
WPI Acc No: 2000-543106/200049
XRPX Acc No: N00-401793

Data network e.g. Internet, intranet, has exposure analysis processor which determines classification of each of unique addresses into groups of unused address, non-shareable and shareable address

Patent Assignee: MCI WORLDCOM INC (MCIW-N)
Inventor: FUDGE B

Number of Countries: 024 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200041059	A1	20000713	WO 99US30211	A	19991217	200049	B
US 6205552	B1	20010320	US 98224132	A	19981231	200118	
EP 1147465	A1	20011024	EP 99966417	A	19991217	200171	
			WO 99US30211	A	19991217		
JP 2002534877	W	20021015	WO 99US30211	A	19991217	200282	
			JP 2000592718	A	19991217		

Priority Applications (No Type Date): US 98224132 A 19981231
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200041059	A1	E	21	G06F-003/00	
Designated States (National): CA JP MX SG					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
US 6205552	B1			G06F-011/30	
EP 1147465	A1	E		G06F-003/00	Based on patent WO 200041059
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
JP 2002534877	W		19	H04L-012/26	Based on patent WO 200041059

Abstract (Basic): WO 200041059 A1

NOVELTY - **Several devices** are connected to a data network, each of which correspond to a unique address in a range of Internet protocol (IP) addresses. An exposure analysis processor determines a classification of each of unique addresses into groups consisting of unused addresses, non-shareable addresses and shareable device addresses.

DETAILED DESCRIPTION - An address database connected to exposure analysis processor, stores the classification determined by exposure analysis processor, for each unique address in the range of IP addresses. A vulnerability scanner selectively scans only the addresses classified as shareable device addresses by exposure analysis processor. An INDEPENDENT CLAIM is also included for scanning method for checking vulnerability of devices in data network.

USE - In Internet, intranet for transporting information via computers, display terminals, routers, printers, hubs.

ADVANTAGE - Since the scanner scans the devices connected to network only for those provided services rather than for all possible services, time and cost in scanning for vulnerable devices are reduced.

DESCRIPTION OF DRAWING(S) - The figure shows a flow chart describing a process for selecting and profiling network addresses as candidates for in-depth vulnerability testing.

pp; 21 DwgNo 2/3

Title Terms: DATA; NETWORK; EXPOSE; ANALYSE; PROCESSOR; DETERMINE; CLASSIFY ; UNIQUE; ADDRESS; GROUP; ADDRESS; NON; ADDRESS

Derwent Class: T01; W01
International Patent Class (Main): G06F-003/00; **G06F-011/30** ; H04L-012/26
International Patent Class (Additional): G06F-012/00; G06F-012/14; G06F-012/16; **G06F-013/00** ; **G06F-013/28** ; G06F-015/16; G06F-015/173; **H04L-009/00** ; **H04L-009/32** ; H04L-012/56
File Segment: EPI
Manual Codes (EPI/S-X): T01-C; T01-G05C; T01-H; T01-H01C2; T01-H01C4; T01-H05B2; T01-H07C7; T01-M02; W01-A05; W01-A05B

44/9/15 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013310566 **Image available**
WPI Acc No: 2000-482503/200042
XRPX Acc No: N00-358747
Computer network penetration **test system for** detecting vulnerabilities **in a network has modules to scan computer to learn unwanted accessing elimination capability of computer**
Patent Assignee: AXENT TECHNOLOGIES INC (AXEN-N)
Inventor: KINGSFORD B; MCQUEEN S; THROWER W A
Number of Countries: 088 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200038036	A2	20000629	WO 99US30850	A	19991222	200042	B
AU 200022138	A	20000712	AU 200022138	A	19991222	200048	
EP 1141831	A2	20011010	EP 99966633	A	19991222	200167	
			WO 99US30850	A	19991222		

Priority Applications (No Type Date): US 98220125 A 19981223
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200038036	A2	E	53	G06F-001/00	
AU 200022138	A			G06F-001/00	Based on patent WO 200038036
EP 1141831	A2	E		G06F-011/14	Based on patent WO 200038036

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

Abstract (Basic): WO 200038036 A2
NOVELTY - The penetration test **system** has scan **modules** (16) to scan network to learn the unwanted accessing elimination capability of the computer. The scan results are stored in the memory. A controller retrieves information from the memory and instructs one scan module to perform scan of the computer and to produce an output, and for producing an input to another scan module based on the output.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(a) method for performing penetration test on a computer network;
(b) signal for performing penetration test
USE - For penetrating computer or a computer network to discover vulnerabilities.
ADVANTAGE - The use of **multiple** scan **modules** allows a complete scan to run more quickly by performing many scanning operations in

parallel. The multilevel approach of scanning is more than simply a parallel processing scheme since it can establish both hierarchies and priorities among the techniques to be run, and it can decide which information to share, thereby improving penetration efficiency and effectiveness.

DESCRIPTION OF DRAWING(S) - The figure shows the general over view of penetration test system.

Module (16)

pp; 53 DwgNo 1/9

Title Terms: COMPUTER; NETWORK; PENETRATE; TEST; SYSTEM; DETECT; NETWORK; MODULE; SCAN; COMPUTER; LEARNING; UNWANTED; ACCESS; ELIMINATE; CAPABLE; COMPUTER

Derwent Class: T01

International Patent Class (Main): G06F-001/00; G06F-011/14

File Segment: EPI

Manual Codes (EPI/S-X): T01-X

44/9/16 (Item 16 from file: 350)

DIALOG(R)File 350:Derwent WPIX

013216031 **Image available**

WPI Acc No: 2000-387905/200033

Related WPI Acc No: 1998-159709; 2001-581878

XRPX Acc No: N00-290349

Remote auditable secure network installation system in financial institution, has nodes each of which automatically communicates with other node, based on stored information

Patent Assignee: ANGEL SECURE NETWORKS INC (ANGE-N)

Inventor: SMITH B H; SMITH F H

Number of Countries: 088 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200029962	A1	20000525	WO 99US27138	A	19991116	200033	B
AU 200016266	A	20000605	AU 200016266	A	19991116	200042	
EP 1131727	A1	20010912	EP 99959005	A	19991116	200155	
			WO 99US27138	A	19991116		
US 6532543	B1	20030311	US 96689767	A	19960813	200321	
			US 98108566	P	19981116		
			US 98108868	P	19981118		
			US 99121959	P	19990225		
			US 99441403	A	19991116		
			US 2000500883	A	20000209		

Priority Applications (No Type Date): US 99121959 P 19990225; US 98108566 P 19981116; US 98108868 P 19981118; US 96689767 A 19960813; US 99441403 A 19991116; US 2000500883 A 20000209

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200029962	A1	E	96	G06F-013/00	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

AU 200016266	A			Based on patent WO 200029962
EP 1131727	A1	E	G06F-013/00	Based on patent WO 200029962

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

US 6532543 B1 H04L-009/00 CIP of application US 96689767
Provisional application US 98108566
Provisional application US 98108868
Provisional application US 99121959
CIP of application US 99441403
CIP of patent US 6067582

Abstract (Basic): WO 200029962 A1

NOVELTY - Installation server (630) does installation of software application on remote computer to form node. A generator (620) generates **several** software **modules** including agent modules which are executed by computer, to communicate with server (630). Each node automatically establishes communication with other node, based on information stored in template (610). A monitor node (670) monitors security of network.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for remote auditable secure network installation method.

USE - For financial institution, for protecting copyrights for security of distributed software over network through Internet.

ADVANTAGE - Prevents unauthorized copying of electronically stored and transmitted data by pirates and trusted insiders. The monitoring capability is used to ensure security maintenance. A set of agent library function is included with application to facilitate communication of each node with the rest of network. When system is installed, the keys are changed or strobe every few seconds, thus substantially diminishes the time during which private keys remain valid and substantially reduces risk of private keys being stolen and used by pirates. Enables to detect theft during relatively brief period when private key is in effect.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of system for generating and installing a private secure audible network.

Template (610)
Generator (620)
Installation server (630)
Monitor node (670)
pp; 96 DwgNo 6A/18

Title Terms: REMOTE; SECURE; NETWORK; INSTALLATION; SYSTEM; FINANCIAL; INSTITUTION; NODE; AUTOMATIC; COMMUNICATE; NODE; BASED; STORAGE; INFORMATION

Derwent Class: T01

International Patent Class (Main): G06F-013/00; **H04L-009/00**

File Segment: EPI

Manual Codes (EPI/S-X): T01-F05B2; **T01-H07C5A** ; **T01-J12C**

44/9/17 (Item 17 from file: 350)

DIALOG(R)File 350:Derwent WPIX

013052597 **Image available**

WPI Acc No: 2000-224452/200019

XRPX Acc No: N00-168180

Security device for multi - level **network** system **has two port RAM consisting two bus interfaces which are** respectively connected to host **bus and local bus**

Patent Assignee: CRYPTEK SECURE COMMUNICATIONS LLC (CRYP-N); CRYPTEK INC (CRYP-N)

Inventor: WILLIAMS T C

Number of Countries: 087 Number of Patents: 008

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week

WO 200010278	A2	20000224	WO 99US16416	A	19990721	200019	B
AU 200015954	A	20000306	AU 200015954	A	19990721	200030	
EP 1101161	A2	20010523	EP 99958627	A	19990721	200130	
			WO 99US16416	A	19990721		
US 6304973	B1	20011016	US 98129879	A	19980806	200164	
ZA 200100540	A	20020626	ZA 2001540	A	20010118	200251	
AU 750858	B	20020801	AU 200015954	A	19990721	200261	
US 20030005331	A1	20030102	US 98129879	A	19980806	200305	
			US 2001933760	A	20010822		
NZ 509570	A	20030328	NZ 509570	A	19990721	200325	
			WO 99US16416	A	19990721		

Priority Applications (No Type Date): US 98129879 A 19980806; US 2001933760 A 20010822

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200010278	A2	E	103	H04L-000/00	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW					
AU 200015954	A			H04L-000/00	Based on patent WO 200010278
EP 1101161	A2	E		G06F-003/00	Based on patent WO 200010278
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
US 6304973	B1			G06F-012/14	
ZA 200100540	A		116	H04L-000/00	
AU 750858	B			G06F-003/00	Previous Publ. patent AU 200015954 Based on patent WO 200010278
US 20030005331	A1			G06F-011/30	Cont of application US 98129879 Cont of patent US 6304973
NZ 509570	A			H04L-009/10	Div in patent NZ 523940 Based on patent WO 200010278

Abstract (Basic): WO 200010278 A2

NOVELTY - A network interface connects the local bus of security device to network such as local area, Ethernet or ring network. A two port RAM has two bus interfaces, which are respectively connected to host bus and local bus such that the host computer and the client computer are connected.

DETAILED DESCRIPTION - An authentication interface is provided to authenticate the user. A CPU is provided for implementing firmware and a cipher unit is connected to the local bus. An INDEPENDENT CLAIM is also included for data transmission and receiving control method.

USE - For **multi - level** network **system** .

ADVANTAGE - Prevents unauthorized access from host computer, since two-port RAM connects host bus and local bus using its two interface, thus security is improved. Reduces problems associated with traditional I and A device, intrusion detectors, firewalls and VPNs and previous MLS networks.

DESCRIPTION OF DRAWING(S) - The figure shows model diagram of secure network having security device.

pp; 103 DwgNo 1/14

Title Terms: SECURE; DEVICE; MULTI; LEVEL; NETWORK; SYSTEM; TWO; PORT; RAM; CONSIST; TWO; BUS; INTERFACE; RESPECTIVE; CONNECT; HOST; BUS; LOCAL; BUS

Derwent Class: T01; W01

International Patent Class (Main): G06F-003/00; **G06F-011/30** ; G06F-012/14; H04L-000/00; **H04L-009/10**

International Patent Class (Additional): **G06F-013/00** ; **H04L-009/00**

File Segment: EPI
Manual Codes (EPI/S-X): **T01-H07C5A** ; **T01-J12C** ; W01-A03A1; W01-A06B2; W01-A06B5A; W01-A06B7; W01-A06G3

44/9/18 (Item 18 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013023262 **Image available**
WPI Acc No: 2000-195113/200017
XRPX Acc No: N00-144389

Network security system **has** modules **monitoring networks to build network and usage maps that are transferred to analytical engines that detect security situations**

Patent Assignee: RAYTHEON CO (RAYT); RAYTHEON CO LTD (RAYT)
Inventor: MALONEY M P; SCOTT C J; SUIT J M; WOODUS F M
Number of Countries: 087 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200005650	A1	20000203	WO 99US16363	A	19990720	200017	B
AU 9951142	A	20000214	AU 9951142	A	19990720	200029	
US 6253337	B1	20010626	US 9893551	A	19980721	200138	
			US 99357539	A	19990719		
TW 470879	A	20020101	TW 99112341	A	19991005	200281	

Priority Applications (No Type Date): US 9893551 P 19980721; US 99357539 A 19990719
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200005650	A1	E	39	G06F-011/00	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

AU 9951142	A	G06F-011/00	Based on patent WO 200005650
US 6253337	B1	G06F-011/30	Provisional application US 9893551
TW 470879	A	G06F-011/30	

Abstract (Basic): WO 200005650 A1

NOVELTY - The information network system has discovery units (12) that passively or actively monitor a network, e.g. a LAN (14). The units build a map of the network and the usage patterns on it and store these in a database (16). This data is extracted by a parsing tool (18) that adapts it for input to analytical engines (20). These detect patterns in the overall network and provide alerts and displays (22,24) to the operator. Additional discovery or analytical modules can be added as they become available.

USE - Analysis and monitoring of networks

ADVANTAGE - Provides a modular system of collecting and analyzing data to detect performance and security issues.

DESCRIPTION OF DRAWING(S) - Network monitoring
Monitoring modules (12)
Database of network and usage (16)
Converter for later engines (18)
Analysis of data (20)
Presentation (22,24)
pp; 39 DwgNo 1/8

Title Terms: NETWORK; SECURE; SYSTEM; MODULE; MONITOR; NETWORK; BUILD;

NETWORK; MAP; TRANSFER; ANALYSE; ENGINE; DETECT; SECURE; SITUATE
Derwent Class: T01
International Patent Class (Main): G06F-011/00; **G06F-011/30**
International Patent Class (Additional): G06F-015/16
File Segment: EPI
Manual Codes (EPI/S-X): T01-G05C; **T01-H07C5A ; T01-J12C**

44/9/19 (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013010925 **Image available**
WPI Acc No: 2000-182777/200016
XRPX Acc No: N00-134743
Network security system **has** modules **monitoring networks to build network and usage maps that are transferred to analytical engines that present security situations**
Patent Assignee: SILENTRUNNER INC (SILE-N); RAYTHEON CO (RAYT)
Inventor: MALONEY M P; RUBEL R; SUIT J M; WOODUS F M
Number of Countries: 088 Number of Patents: 011
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200005651	A1	20000203	WO 99US16467	A	19990720	200016	B
AU 9951174	A	20000214	AU 9951174	A	19990720	200029	
NO 200100339	A	20010306	WO 99US16467	A	19990720	200123	
			NO 2001339	A	20010119		
EP 1097420	A1	20010509	EP 99935767	A	19990720	200128	
			WO 99US16467	A	19990720		
US 6269447	B1	20010731	US 9893559	P	19980721	200146	
			US 99358131	A	19990719		
BR 9912192	A	20010925	BR 9912192	A	19990720	200161	
			WO 99US16467	A	19990720		
KR 2001079561	A	20010822	KR 2001701041	A	20010122	200213	
JP 2002521748	W	20020716	WO 99US16467	A	19990720	200261	
			JP 2000561559	A	19990720		
TW 476204	A	20020211	TW 99112343	A	19991005	200304	
NZ 509606	A	20030131	NZ 509606	A	19990720	200319	
			WO 99US16467	A	19990720		
AU 756407	B	20030109	AU 9951174	A	19990720	200320	

Priority Applications (No Type Date): US 9893559 P 19980721; US 99358131 A 19990719
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200005651	A1	E	39	G06F-011/00	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW					
AU 9951174	A			G06F-011/00	Based on patent WO 200005651
NO 200100339	A			G06F-000/00	
EP 1097420	A1	E		G06F-011/00	Based on patent WO 200005651
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
US 6269447	B1			G06F-011/00	Provisional application US 9893559
BR 9912192	A			G06F-011/00	Based on patent WO 200005651
KR 2001079561	A			G06F-015/00	
JP 2002521748	W		39	G06F-011/00	Based on patent WO 200005651

TW 476204	A	H04L-012/00	
NZ 509606	A	G06F-011/00	Based on patent WO 200005651
AU 756407	B	G06F-011/00	Previous Publ. patent AU 9951174 Based on patent WO 200005651

Abstract (Basic): WO 200005651 A1

NOVELTY - The information network system has discovery units (12) that passively or actively monitor a network, e.g. a LAN (14). The units build a map of the network and the usage patterns on it and store these in a database (16). This data is extracted by a parsing tool (18) that adapts it for input to analytical engines (20). These detect patterns in the overall network and provide alerts and displays (22,24) to the operator. Additional discovery or analytical modules can be added as they become available.

USE - Analysis and monitoring of networks

ADVANTAGE - Provides a modular system of collecting and analyzing data to detect performance and security issues.

DESCRIPTION OF DRAWING(S) - Network monitoring

Monitoring modules (12)

Database of network and usage (16)

Converter for later engines (18)

Analysis of data (20)

Presentation (22,24)

pp; 39 DwgNo 1/8

Title Terms: NETWORK; SECURE; SYSTEM; MODULE; MONITOR; NETWORK; BUILD; NETWORK; MAP; TRANSFER; ANALYSE; ENGINE; PRESENT; SECURE; SITUATE

Derwent Class: T01

International Patent Class (Main): G06F-000/00; G06F-011/00; G06F-015/00; H04L-012/00

International Patent Class (Additional): G06F-003/00; G06F-009/445; G06F-009/45; **G06F-011/30** ; G06F-013/00; H04L-012/66; H04L-029/06

File Segment: EPI

Manual Codes (EPI/S-X): T01-H01C2; **T01-H07C5A** ; T01-H07C5E; **T01-J12C** ; T01-J16C

44/9/20 (Item 20 from file: 350)

012915661 **Image available**

WPI Acc No: 2000-087497/200007

Related WPI Acc No: 1999-561717

XRPX Acc No: N00-068688

Security system for business use computer

Patent Assignee: DMW WORLDWIDE INC (DMWW-N); HARTLEY B V (HART-I); KNIGHT E (KNIG-I); MAVROS C (MAVR-I); REYNOLDS K (REYN-I); ZYMBALUK G (ZYMB-I)

Inventor: HARTLEY B V; KNIGHT E; MAVROS C; REYNOLDS K; ZYMBALUK G

Number of Countries: 084 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9966383	A2	19991223	WO 99US13476	A	19990615	200007 B
AU 9945682	A	20000105	AU 9945682	A	19990615	200024
US 20020026591	A1	20020228	US 9891270	P	19980615	200220
			US 99333547	A	19990615	
			US 2001834334	A	20010412	

Priority Applications (No Type Date): US 9891270 P 19980615; US 99333547 A 19990615; US 2001834334 A 20010412

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes

WO 9966383 A2 E 37 G06F-000/00
Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW
AU 9945682 A G06F-000/00 Based on patent WO 9966383
US 20020026591 A1 G06F-011/30 Provisional application US 9891270

Cont of application US 99333547

Abstract (Basic): WO 9966383 A2

NOVELTY - Security **module** of the **system** under direction from processor (12) accesses and analyzes selected portions of the computer comprising unix server (10) to identify vulnerabilities. Utility module under direction from processor performs various utility functions with regard to computer, in response to identified vulnerabilities.

DETAILED DESCRIPTION - Security information for performing analysis of computer is stored in security system memory (30). The security system is connected to the computer comprising unix server (10) via (18). The reporting **module** of the **system** provides status information to GUI with regard to operations of the **system** . The security **module** includes at least one of configuration mode which performs initial analysis of the computer system acquire configuration information, directory checking module analyzing directories and files in system memory (13) to determine if security initial files have been tampered, user manager module, integrity checking module, network checking module and a password checking module. The utility module is chosen from user manager module, file removal module, file marking module, and scheduling module. An INDEPENDENT CLAIM is also included for method of providing a security assessment for computer system.

USE - For business use computer.

ADVANTAGE - Enables manually marking certain critical files and analyzing the marked files to detect tampering when directory check module is activated. Enables scheduling automated performance of functions and providing reports to the system user in a number of different formats.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of security system.

Unix server (10)
Processor (12)
System memory (13)
Via (18)
Security system memory (30)
pp; 37 DwgNo 1/15

Title Terms: SECURE; SYSTEM; BUSINESS; COMPUTER
Derwent Class: T01
International Patent Class (Main): G06F-000/00; **G06F-011/30**
International Patent Class (Additional): **H04L-009/00**
File Segment: EPI
Manual Codes (EPI/S-X): **T01-H07C5A** ; **T01-J12C**

44/9/21 (Item 21 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012883691 **Image available**
WPI Acc No: 2000-055524/200005
XRPX Acc No: N00-043409

Permit method for controlling access to services in protected memory

Patent Assignee: SUN MICROSYSTEMS INC (SUNM)
Inventor: GOLDSTEIN T C; LIPKIN E
Number of Countries: 029 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 965917	A1	19991222	EP 99201908	A	19990615	200005	B
CN 1239787	A	19991229	CN 99109092	A	19990618	200019	
JP 2000057045	A	20000225	JP 99169025	A	19990615	200021	
US 6131165	A	20001010	US 9899579	A	19980618	200052	
SG 76624	A1	20001121	SG 992860	A	19990603	200067	

Priority Applications (No Type Date): US 9899579 A 19980618
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 965917	A1	E	16	G06F-009/46	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
CN 1239787	A			G06F-013/16	
JP 2000057045	A		15	G06F-012/00	
US 6131165	A			G06F-011/30	
SG 76624	A1			G06F-015/163	

Abstract (Basic): EP 965917 A1

NOVELTY - The computer **system** allows **modules** to be transferred to other computers, e.g. via Java(TM) modules and interact with services on that computer. The client code uses established systems to obtain permission to access services and is provided with a permit object to reflect this. The client invokes methods on this object (502) and the system checks the validity (504). If valid the controlled object is invoked. Both permit and controlled objects are in protected memory spaces.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for:

(1) a computer readable medium containing program instructions; and

(2) an apparatus for controlling access to services in a protected memory system.

USE - Access control for use of computer services

ADVANTAGE - Does not require extra hardware to control access to services

DESCRIPTION OF DRAWING(S) - Access control

Client code invokes permit object to access restricted services (502)

System validates call (504)

Controlled object invoked if call valid (506-508)

pp; 16 DwgNo 5/5

Title Terms: PERMIT; METHOD; CONTROL; ACCESS; SERVICE; PROTECT; MEMORY
Derwent Class: P85; T01
International Patent Class (Main): G06F-009/46; **G06F-011/30** ; G06F-012/00; **G06F-013/16** ; G06F-015/163
International Patent Class (Additional): G06F-001/00; G06F-012/14; **G06F-013/28** ; G09C-001/00; **H04L-009/32**
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-F07; T01-H01C; T01-H07C3E; T01-S03

44/9/22 (Item 22 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012807057 **Image available**

WPI Acc No: 1999-613287/199953
XRPX Acc No: N99-452168

Computer network devices security system for e.g. prevents unauthorized removal of network devices

Patent Assignee: 3COM CORP (THRE-N); 3COM TECHNOLOGIES (THRE-N)
Inventor: LOCKYER T D; LOCKYER T
Number of Countries: 020 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2337840	A	19991201	GB 9912613	A	19990528	199953	B
WO 9963726	A1	19991209	WO 99IB1384	A	19990528	200005	
US 6064305	A	20000516	US 98113782	A	19980710	200031	
GB 2337840	B	20000726	GB 9912613	A	19990528	200037	

Priority Applications (No Type Date): GB 9811641 A 19980529
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2337840	A		20	G08B-013/14	
WO 9963726	A1	E		H04L-029/06	
Designated States (National): GB JP					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
US 6064305	A			G08B-013/22	
GB 2337840	B			G08B-013/14	

Abstract (Basic): GB 2337840 A

NOVELTY - A communication hub (10) comprises **several devices** (20) connected to ports (12) by cables (16), with detection switches (22) allowing the monitoring (14) of the devices. A management device (20a) indicates which device is to be monitored and an alarm (27) associated with a control device (26), is arranged to give an indication if it is determined that a network device which is currently subject to monitoring is removed.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) a computer monitoring system and

(2) a computer network device.

USE - For the security of network devices within a computer network i.e. prevents unauthorized removal of network devices.

ADVANTAGE - Network devices are able to be 'locked' onto the network with an alarm raised if the device is removed even when the device is switched off, as the monitoring of the device's presence is performed by the network. The device may be 'unlocked' from the network, in which condition no alarm is raised even if the device is removed. Control of whether a particular network device is subject to the alarm system is therefore in the hands of the user of the device, and is particularly useful for items such as laptop computers which may quite legitimately be regularly connected/disconnected from the network. No additional circuitry is required, as the alarm utilizes the data cables which removes any need for specific cable installation.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic illustration of the network.

Communication hub (10)
Ports (12)
Monitoring (14)
Cables (16)
Network devices (20)
Management device (20a)
Detection switches (22)
Control device (26)
Alarm (27)

pp; 20 DwgNo 1/2
Title Terms: COMPUTER; NETWORK; DEVICE; SECURE; SYSTEM; PREVENT; REMOVE; NETWORK; DEVICE
Derwent Class: T01; W05
International Patent Class (Main): G08B-013/14; G08B-013/22; H04L-029/06
International Patent Class (Additional): G06F-001/00; G08B-025/08; H04L-012/24; H04L-012/26; H04L-012/44
File Segment: EPI
Manual Codes (EPI/S-X): **T01-H07C5A** ; T01-J05A2; **T01-J12C** ; W05-B01B; W05-B05B9; W05-C02

44/9/23 (Item 23 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012745414 **Image available**
WPI Acc No: 1999-551531/199946
XRPX Acc No: N99-408081
Network service provision method using common interface
Patent Assignee: OMNES (OMNE-N)
Inventor: CUMMINGHAM C M; CUNNIHAM C M
Number of Countries: 083 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9946692	A2	19990916	WO 99US4699	A	19990303	199946	B
AU 9929815	A	19990927	AU 9929815	A	19990303	200006	
EP 1064755	A2	20010103	EP 99911088	A	19990303	200102	
			WO 99US4699	A	19990303		
BR 9909649	A	20020305	BR 999649	A	19990303	200225	
			WO 99US4699	A	19990303		

Priority Applications (No Type Date): US 9842338 A 19980313
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9946692	A2	E	26	G06F-017/00	
Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW					
AU 9929815	A			G06F-017/00	Based on patent WO 9946692
EP 1064755	A2	E		H04L-012/24	Based on patent WO 9946692
Designated States (Regional): DE FR GB					
BR 9909649	A			G06F-017/00	Based on patent WO 9946692

Abstract (Basic): WO 9946692 A2

NOVELTY - A graphical user interface that allows a client to request, via a computer, information about the client's network from any of the dedicated service machines, is presented. Requested information is retrieved from an appropriate dedicated service machine. Requested information is shown to the client via the graphical user interface.

USE - For providing network administration services executed by dedicated service machines executing special purpose programs in computer network maintained by service provider, to remote client computer.

ADVANTAGE - Allows client to access information immediately via the computer without submitting requests to human operators and await human action for responses to the requests. Eliminates need for client to

purchase or understand hardware and software components used to provide the network management service. Network owner can **outsource** all network management responsibilities without forfeiting quick and easy access to information about network, and can receive quick and easy-to-understand reports on service provider's performance.

DESCRIPTION OF DRAWING(S) - The figure shows a schematic diagram of the computer network that provides network services to a remote client computer.

pp; 26 DwgNo 1/5

Title Terms: NETWORK; SERVICE; PROVISION; METHOD; COMMON; INTERFACE

Derwent Class: T01; W01

International Patent Class (Main): G06F-017/00; H04L-012/24

File Segment: EPI

Manual Codes (EPI/S-X): T01-H07C5; **T01-H07C5A** ; T01-J05B; **T01-J12C** ; T01-M02A1B; W01-A06B7

44/9/27 (Item 27 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011931972 **Image available**
WPI Acc No: 1998-348882/199830
Related WPI Acc No: 1998-532210
XRPX Acc No: N98-272277

Distributed remote monitoring method for network traffic and performance use between several devices **- using distributed nodes on network to collect traffic statistics, compiling data to generate combined view of network, and forwarding performance data to network manager**

Patent Assignee: 3COM CORP (THRE-N)
Inventor: BANTHIA P; FLETCHER R; BANTHIA P C; LIN P

Number of Countries: 021 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9826541	A1	19980618	WO 97US22816	A	19971212	199830 B
AU 9856011	A	19980703	AU 9856011	A	19971212	199847
US 5922044	A	19990713	US 96766274	A	19961213	199934
			US 9740876	A	19970321	
			US 97873440	A	19970612	
GB 2335124	A	19990908	WO 97US22816	A	19971212	199938
			GB 9913682	A	19990611	
EP 956680	A1	19991117	EP 97952393	A	19971212	199953
			WO 97US22816	A	19971212	
US 6009274	A	19991228	US 96766274	A	19961213	200007
			US 9740876	A	19970321	
			US 97881517	A	19970624	
US 6085243	A	20000704	US 96766274	A	19961213	200036
US 6108782	A	20000822	US 96766274	A	19961213	200042
			US 9740876	A	19970321	
			US 97882207	A	19970624	

Priority Applications (No Type Date): US 9740876 P 19970321; US 96766274 A 19961213; US 97873440 A 19970612; US 97881517 A 19970624; US 97882207 A 19970624

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9826541	A1	E	55	H04L-012/24	
Designated States (National): AU CA GB					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
AU 9856011	A			H04L-012/24	Based on patent WO 9826541
US 5922044	A			G06F-013/00	CIP of application US 96766274 Provisional application US 9740876
GB 2335124	A			H04L-012/26	Based on patent WO 9826541
EP 956680	A1	E		H04L-012/24	Based on patent WO 9826541
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
US 6009274	A			G06F-009/445	CIP of application US 96766274 Provisional application US 9740876
US 6085243	A			G06F-017/00	
US 6108782	A			H04L-009/00	CIP of application US 96766274 Provisional application US 9740876

Abstract (Basic): WO 9826541 A

The method for distributed collecting of network statistics involves gathering network statistics at a number of nodes in the network. Data containing the statistics is transmitted to a collector.

The statistics from the nodes are combined to form group network statistics. Network performance data is reported based on the compiled statistics from the data collector to a network manager.

Values are set at the collector to configure the collecting of the network statistics. The configuration data is forwarded by the collector to the nodes to configure the data gathering at the nodes. An agent is launched in the nodes participating in the distributed collecting, and an agent is an executable module for gathering statistics and communicating with the collector.

USE - E.g. for communications systems for CATV, ATM data transfer and advanced telephony. Is particularly suited to LAN environment with end systems running under Windows-compatible network operating system.

ADVANTAGE - Is usable with variety of standard network management protocols such as simple network management protocol (SNMP), remote monitoring systems RMON and RMON2.

Dwg.1/10

Title Terms: DISTRIBUTE; REMOTE; MONITOR; METHOD; NETWORK; TRAFFIC; PERFORMANCE; DEVICE; DISTRIBUTE; NODE; NETWORK; COLLECT; TRAFFIC; STATISTICAL; COMPILE; DATA; GENERATE; COMBINATION; VIEW; NETWORK; FORWARDING; PERFORMANCE; DATA; NETWORK; MANAGE

Derwent Class: T01; W01

International Patent Class (Main): G06F-009/445; **G06F-013/00** ; G06F-017/00 ; **H04L-009/00** ; H04L-012/24; H04L-012/26

International Patent Class (Additional): **G06F-011/30**

File Segment: EPI

Manual Codes (EPI/S-X): T01-M02A1; W01-A06A; W01-A06B5A; W01-A06F

File 347:JAPIO Oct 1976-2002/Dec(Updated 030402)
(c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200328
(c) 2003 Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2003/Apr W03
(c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20030501,UT=20030424
(c) 2003 WIPO/Univentio
? ds

Set	Items	Description
S1	4	AU='HRABIK M':AU='HRABIK MICHAEL'
S2	2	AU='GUILFOYLE J':AU='GUILFOYLE J J'
S3	2	AU='GUILFOYLE JEFFREY'
S4	1	AU='MAC BEAVER E'
S5	5	AU='BEAVER E':AU='BEAVER E R'
S6	2	AU='BEAVER EDWARD MAC'
S7	4	S1 AND S2:S3 AND S4:S6
S8	8	S1:S6
S9	5144	COMPUTER(3N)(SECURITY OR COUNTERMEASUR? OR COUNTER)
S10	3	S8 AND S9
S11	4	S7 OR S10

? t11/9/1-2

11/9/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015215025 **Image available**
WPI Acc No: 2003-275562/200327
Related WPI Acc No: 2003-057189
XRPX Acc No: N03-218808

Computer security **system has log analyzer which analyzes event messages received from network devices and uploads to security master system when security threat is found**

Patent Assignee: GUILFOYLE J (GUIL-I); HRABIK M (HRAB-I); MAC BEAVER E (BEAV-I)
Inventor: **GUILFOYLE J ; HRABIK M ; MAC BEAVER E**
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020178383	A1	20021128	US 2001770525	A	20010125	200327	B
			US 2002196472	A	20020716		

Priority Applications (No Type Date): US 2002196472 A 20020716; US 2001770525 A 20010125
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020178383	A1		14	G06F-011/30	CIP of application US 2001770525

Abstract (Basic): US 20020178383 A1

NOVELTY - A security subsystem (50) associated with the computer has a collection engine (502) which collects the event messages from the target network, and stores in an event log (512). A log analyzer (504) analyzes the event messages and when any of the event is determined to be a security threat or a high priority event, it is uploaded to a security master system (60) through a secure link.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) network security system;

(2) method for monitoring the integrity of computer; and

(3) method for monitoring the integrity of target computer network.

USE - **Computer security** system.

ADVANTAGE - Provides security for the resources that interact with customers, employees and partners over the internet.

DESCRIPTION OF DRAWING(S) - The figure shows a flowchart explaining the steps of verifying the integrity of computer networks.

security subsystem (50)

security master system (60)

collection engine (502)

log analyzer (504)

event log (512)

pp; 14 DwgNo 4/4

Title Terms: COMPUTER; SECURE; SYSTEM; LOG; ANALYSE; ANALYSE; EVENT; MESSAGE; RECEIVE; NETWORK; DEVICE; SECURE; MASTER; SYSTEM; SECURE; THREAT ; FOUND

Derwent Class: T01

International Patent Class (Main): G06F-011/30

File Segment: EPI

Manual Codes (EPI/S-X): T01-N02B2B

11/9/2 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014996674 **Image available**

WPI Acc No: 2003-057189/200305

Related WPI Acc No: 2003-275562

XRPX Acc No: N03-044246

Computer **network** security **system monitors security subsystem through secure link, and registers information pertaining to attacks detected by subsystem**

Patent Assignee: BEAVER E M (BEAV-I); GUILFOYLE J J (GUIL-I); HRABIK M (HRAB-I); SOLUTIONARY INC (SOLU-N)

Inventor: **BEAVER E M ; GUILFOYLE J J ; HRABIK M ; GUILFOYLE J**

Number of Countries: 097 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020099958	A1	20020725	US 2001770525	A	20010125	200305	B
WO 200260117	A1	20020801	WO 2002US2218	A	20020124	200305	

Priority Applications (No Type Date): US 2001770525 A 20010125

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020099958	A1		7	G06F-011/30	
WO 200260117	A1	E		H04L-009/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

Abstract (Basic): US 20020099958 A1

NOVELTY - A security subsystem linked to each of computers in a target network (100) by a secure link (52), detects attack on the computer. A secure link (54) is provided between the security subsystem and a master system (60) connected to a remote network (110). The master system registers information pertaining to attacks detected by the security subsystem.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for a method for monitoring integrity of security subsystem associated with a target network.

USE - **Computer** network **security** system.

ADVANTAGE - By providing a secure link which ensures that communication between the two networks cannot be intercepted by an intruder, even if completely subverted during an attack on target network, the security subsystem will still be able to carry out its function. Enables to detect easily signs of intruder activity on a network and hence resist intrusion during an attack on the network.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of a network incorporating a security system.

Secure links (52,54)
Master system (60)
Target network (100)
Remote network (110)
pp; 7 DwgNo 2/2

Title Terms: COMPUTER; NETWORK; SECURE; SYSTEM; MONITOR; SECURE; SUBSYSTEM; THROUGH; SECURE; LINK; REGISTER; INFORMATION; PERTAIN; ATTACK; DETECT; SUBSYSTEM
Derwent Class: T01
International Patent Class (Main): G06F-011/30; H04L-009/00
File Segment: EPI
Manual Codes (EPI/S-X): T01-N02B; T01-N02B2
? t11/5/3-4

11/5/3 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2003 European Patent Office. All rts. reserv.

01454439
METHOD AND APPARATUS FOR VERIFYING THE INTEGRITY OF COMPUTER NETWORKS AND IMPLEMENTATION OF COUNTER MEASURES
PROCEDE ET APPAREIL DE VERIFICATION DE L'INTEGRITE DES RESEAUX INFORMATIQUES ET MISE EN OEUVRE DE CONTREMESURES
PATENT ASSIGNEE:
Solutionary, Inc., (4175320), 9420 Underwood Avenue, Ohama, NE 68114, (US), (Applicant designated States: all)
INVENTOR:
HRABIK, Michael , 9420 Underwood Avenue, Omaha, NE 68114, (US)
GUILFOYLE, Jeffrey , 9420 Underwood Avenue, Omaha, NE 68114, (US)
BEAVER, Edward, Mac , 9420 Underwood Avenue, Omaha, NE 68114, (US
PATENT (CC, No, Kind, Date): WO 2002060117 020801
APPLICATION (CC, No, Date): EP 2002709175 020124; WO 2002US2218 020124
PRIORITY (CC, No, Date): US 770525 010125
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/00
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020925 A1 International application. (Art. 158(1))
Application: 020925 A1 International application entering European phase
LANGUAGE (Publication,Procedural,Application): English; English; English

11/5/4 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2003 WIPO/Univentio. All rts. reserv.

00926001 **Image available**

METHOD AND APPARATUS FOR VERIFYING THE INTEGRITY OF COMPUTER NETWORKS AND IMPLEMENTATION OF COUNTER MEASURES

PROCEDE ET APPAREIL DE VERIFICATION DE L'INTEGRITE DES RESEAUX INFORMATIQUES ET MISE EN OEUVRE DE CONTREMESURES

Patent Applicant/Assignee:
SOLUTIONARY INC, 9420 Underwood Avenue, Omaha , NE 68114, US, US (Residence), US (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:
HRABIK Michael , 9420 Underwood Avenue, Omaha, NE 68114, US, US (Residence), US (Nationality), (Designated only for: US)
GUILFOYLE Jeffrey , 9420 Underwood Avenue, Omaha, NE 68114, US, US (Residence), US (Nationality), (Designated only for: US)
BEAVER Edward Mac , 9420 Underwood Avenue, Omaha, NE 68114, US, US (Residence), US (Nationality), (Designated only for: US

Legal Representative:
ANGOTTI Donna L (agent), Schulte Roth & Zabel, LLP, 919 Third Avenue, New York, NY 10022, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200260117 A1 20020801 (WO 0260117)
Application: WO 2002US2218 20020124 (PCT/WO US0202218)
Priority Application: US 2001770525 20010125

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW (EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

Main International Patent Class: H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 3843

English Abstract
A method and apparatus for verifying the integrity of devices on a target network (100) having two components: a subsystem (50) connected to the target network (100), and a master system (60), isolated therefrom by a secure lin (52). The topological and hierarchical relationship of the devices to each other improves stability of the apparatus. Random testing of the subsystem (50) by the master system (60) provide verification and independent self-checking.

French Abstract
La presente invention concerne un procede et un appareil de verification de l'integrite de dispositifs sur un reseau cible (100) possedant deux composants : un sous-systeme (50) connecte au reseau cible (100) et un systeme principal (60), isole par une liaison sure (52). La relation topologique et hierarchique desdits dispositifs les uns par rapport aux autres ameliore la stabilite de l'appareil. Le test aleatoire du sous-systeme (50) par le systeme principal (60) permet la verification et l'auto-controle independant.

Legal Status (Type, Date, Text)
Publication 20020801 A1 With international search report.
Publication 20020801 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20021227 Request for preliminary examination prior to end of

19th month from priority date

```
File 696:DIALOG Telecom. Newsletters 1995-2003/May 05
         (c) 2003 The Dialog Corp.
File  15:ABI/Inform(R) 1971-2003/May 03
         (c) 2003 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2003/Mar
         (c) 2003 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2003/Apr W4
         (c) 2003 ProQuest
File 553:Wilson Bus. Abs. FullText 1982-2003/Mar
         (c) 2003 The HW Wilson Co
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2003/May 06
         (c) 2003 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2003/May 06
         (c) 2003 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2003/May 06
         (c) 2003 Business Wire.
File 369:New Scientist 1994-2003/Apr W3
         (c) 2003 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2003/May 06
         (c) 2003 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2003/May 05
         (c) 2003 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2003/May 05
         (c) 2003 San Jose Mercury News
File 647:CMP  Computer Fulltext 1988-2003/Apr W2
         (c) 2003 CMP Media, LLC
File 674:Computer News Fulltext 1989-2003/Apr W4
         (c) 2003 IDG Communications
? ds

Set     Items   Description
S1    3730563   INTRUS????? ? OR INTRUD???? ? OR ATTACK???? ? OR PSEUDOATT-
              ACK? OR VULNERAB? OR HACK???? ? OR CRACK???? ? OR MALICIOUS OR
               UNAUTHORIZ? OR UNAUTHORIS? OR INFILTRAT? OR THREAT?
S2    4177150   SECURITY
S3      28512   IDS
S4     569579   PENETRAT? OR BREACH?
S5     121813   S1:S4(3N)(TRACK? OR DETECT? OR MONITOR? OR DISCERN? OR GAU-
              G??? ? OR EXPOS???? ? OR CHECK??? ? OR CHEQU??? ? OR DIAGNOS?-
              ?? ?)
S6      73718   S1:S4(3N)(SELFTEST? OR SELFDIAGNOS? OR DX OR PROBE? ? OR P-
              ROBING? OR ANALYS? OR ANALYZ? OR ANALYT? OR ASSESS????? ? OR -
              BIST)
S7      48121   S1:S4(3N)(EVALUAT? OR SENS?R? ? OR SENSING OR SENSE? ? OR -
              SCREEN?)
S8      20008   NOC OR NETWORK? ?(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CEN-
              TER? ? OR CENTRE? ?)
S9      47745   SOC OR SECURITY(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CENTE-
              R? ? OR CENTRE? ?)
S10   7438482   SYSTEM? ?
S11    287479   S10(3N)(INTEGRATED OR MASTER OR PRINCIPAL OR MAIN OR PARENT
               OR HIERARCH? OR TOPOLOG? OR PRIMARY)
S12     81023   SUBSYSTEM? OR SUB()SYSTEM?
S13      5068   S10(3N)(MULTI()(LAYER? OR LEVEL? OR TIER? OR STACK? OR BRA-
              NCH?) OR MULTILAYER? OR MULTILEVEL? OR MULTITIER? OR MULTISTA-
```

```
            CK? OR MULTIBRANCH?)
S14       1831   S10(3N)(MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIP-
                 LE OR MULTIPLICIT? OR MULTITUD? OR ADDITIONAL)(1W)(LAYER? OR -
                 LEVEL? OR TIER? OR STACK? OR BRANCH?)
S15     210354   FIREWALL? OR FIRE()WALL? ? OR ROUTER? ? OR S3
S16        117   MULTIDEVICE?
S17      33175   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
                 ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
                 VARIOUS OR VARIETY)(1W)DEVICE?
S18     325112   OUTSOURC? OR OUT()SOURC??? ?
S19        746   S5:S7(S)S8:S9
S20       2289   S5:S7(S)(S11:S14 OR SUBCOMPONENT? OR SUBMODULE? OR S10(3N)-
                 (COMPONENT? OR MODULE?))
S21      52310   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
                 ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
                 VARIOUS OR VARIETY)(1W)(COMPONENT? OR MODULE?)
S22        737   S19:S20(S)(S15:S18 OR S21)
S23        142   S19:S20(S)(S16:S18 OR S21)
S24         80   S23/2001:2003
S25         62   S23 NOT S24
S26         53   RD (unique items)
```

26/3,K/2 (Item 2 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00625354
NETSOLVE HITS MARKET WITH NEW MANAGED FIREWALL SERVICE
MANAGED NETWORK SERVICES NEWS
September 23, 1998 VOL: 2 ISSUE: 19 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 795 RECORD TYPE: FULLTEXT

TEXT:
...Secure Managed Firewall, a network
security service designed to compliment NetSolve's existing ProWatch Secure **Intrusion Detection** and Response service. The combination of the two services is part of its strategy to...

...Turner continues. "A year ago analysts were advising companies that security was too strategic to **outsource** to someone else. Now, [business consultants] like the Gartner Group are saying if it is not strategic to a business and not a core competency, then you should **outsource** it."
...Inside The ProWatch Secure Managed Firewall

The ProWatch Secure Managed Firewall is designed for...

...Cisco PIX, and begins 7
days-a-week, 24 hours-a-day monitoring from a **network operation center**

located in Austin, Texas. From information provided by the firewall, NetSolve technicians give real-time...

...systems can be used on a client PC to access and configure the firewall.

...Keeping **Track** Of **Track Intruders**

NetSolve's **intrusion detection** service, ProWatch Secure **Intrusion Detection** and Response, was launched about two years ago, Turner says. "We realized we didn't...NetSolve uses NetRanger security software from The WheelGroup, a
subsidiary of Cisco Systems, for its **intrusion detection** service. NetRanger runs on the UNIX operating system.
"The **intrusion detection** service looks at the packets in a network to determine [what] it is and where...

...the network the
attack is originating from. With the combination of the managed firewall plus **intrusion detection** , you get a good level of security," Turner says.
"This is an outstanding product for...

...NetSolve has tried to move beyond the basic firewall by offering both a firewall and **intrusion detection** service," Kovar adds. "GTE Internetworking [GTE] is one of the only other players in the...

26/3,K/3 (Item 3 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00622599
Products: NetSolve Launches Firewall Service
ISP BUSINESS NEWS
September 7, 1998 VOL: 4 ISSUE: 35 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 301 RECORD TYPE: FULLTEXT

TEXT:
...for the price of one.
The complete suite of services from NetSolve also includes an **intrusion detection** solution/response service. The managed firewall service, which allows only authorized users to enter a network, is based on Cisco's [CSCO] PIX firewall. The **intrusion detection** and response service is based on Cisco's Netranger, allowing NetSolve to monitor the content...

...295/month per firewall for the first line, and $895 for each additional one. The **intrusion detection** and response system alone is $1,495/month for three years, or $700 if deployed...
...FON]
customer would pay for just a managed firewall package.
"The reason why firewall and **intrusion detection** and response services are priced differently is because some companies already have staff trained to...

...either maintain
their own personnel to run firewalls and constantly monitor the data flow, or **outsource** .
This, Turner says, is where ISPs come in - as companies that can private-label NetSolve...

...its network will be
watched 24/7 by personnel of NetSolve's Austin, Texas-based **NOC** .
(Michael Turner, NetSolve, 512/340-3061)
...

26/3,K/6 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02081480 61043016
Locking the doors
Savage, Marcia
Computer Reseller News n913 PP: 72-75 Sep 25, 2000
ISSN: 0893-8377 JRNL CODE: CRN
WORD COUNT: 1889

...TEXT: high-caliber employees watch monitors all day, and are finding it makes more sense to **outsource** that management. For those clients, the Salinas Group provides managed network security through ManagedFirewall.com, which offers realtime **intrusion detection** and 24x7 **monitoring** from its **network operations center** .

Salinas is not alone. Other solution providers that specialize in information security now include managed...

26/3,K/19 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire

1148160
Companies Exhibit the High Tech, Crime-Fighting Tools For 'Fraud in a Brave New World' in Orlando Sept. 30 - Oct. 2, 1997

DATE: September 4, 1997 09:50 E.T. WORD COUNT: 2,842

...Fraud Exhibitor Locator. Contact: Heidi Fincken ad 202-785-0081.

WheelGroup Corp. presents NetRanger(TM) **intrusion detection** system, using the next generation of computer **security** technology for **intrusion detection** and response, while promoting an open systems environment. When the content or context of network...

... Nortel Passport switches, or StorageTek BorderGuard devices. Real-time monitoring of the system can be **outsourced** to a third party or conducted within an organization's own **network operations center** using HP OpenView or IBM NetView network management systems. Contact: Doug Webster at 210-494...

26/3,K/20 (Item 1 from file: 613)
DIALOG(R)File 613:PR Newswire

00466761 20001122DCW008 (USE FORMAT 7 FOR FULLTEXT)
Eurosigncard And Cyber Security, Inc. Agree to Secure And Protect Information Technology in The European Union
PR Newswire
Wednesday, November 22, 2000 09:03 EST
JOURNAL CODE: PR NEWSWIRE, INTERACTIVE CONNECTION LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 385

...services to Fortune(TM) 1000 clients. Its Managed Security Service (MSS) product is a completely **outsourced** suite of perimeter security services
including Virtual Private Networking, **Intrusion Detection** Systems, Anti-Virus,
Firewall, and **Vulnerability Assessment** . Founded in 2000, Cyber Security
operates a full-time **Security Operations Center** (**SOC**) to monitor its
customer's networks.
SOURCE Cyber Security, Inc.
CONTACT: Stephen Quinn, Vice President...

26/3,K/21 (Item 2 from file: 613)
DIALOG(R)File 613:PR Newswire

00436636 20001016HSM035 (USE FORMAT 7 FOR FULLTEXT)
Internet Security Systems And Computacenter Form An Alliance to Launch A New Enterprise Wide Managed Security Service

PR Newswire
Monday, October 16, 2000 06:57 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,169

...security services through partners and service
providers is key to our leadership."

The ability to **outsource** and engage with a trusted managed security services provider helps companies save time and reduces costs in hiring scarce
security resources to **monitor** business critical networks 24 hours a day,
365 days a year. Since 1994, ISS has been offering remote security management
through its **Security Operations Centers** (SOCs), assuring companies that their
networks are being pro-actively monitored and responses initiated by...

...the X-Force(TM), an innovative
research and development team that is constantly working to **detect** and fix
global **security** breaches.

"The reality is that few companies realize how vulnerable they are to attack, and...

26/3,K/22 (Item 3 from file: 613)
DIALOG(R)File 613:PR Newswire

00436634 20001016HSM036 (USE FORMAT 7 FOR FULLTEXT)
Lucent Technologies And Internet Security Systems to Provide Managed Security Services to Emerging Class of 'Cybercarriers'
PR Newswire
Monday, October 16, 2000 06:58 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 824

...to focus on their core
business while trusting their security to experts who conduct 24x7 **security**
monitoring and management of their networks from technically advanced **Security**
Operations Centers (SOCs). ISS managed security services ensure customers'
peace of mind with the ability to **outsource** the management of their information security ensuring around-the-clock, remote information protection
by security...

26/3,K/23 (Item 4 from file: 613)
DIALOG(R)File 613:PR Newswire

00106330 19990511SFTU023 (USE FORMAT 7 FOR FULLTEXT)

WatchGuard Showcases LiveSecurity Broadcast Service at N+I
PR Newswire
Tuesday, May 11, 1999 08:05 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 629

...working with systems security since 1984.

The WatchGuard LiveSecurity Family of Solutions
The WatchGuard LiveSecurity **System** delivers the **components** designed to
protect companies conducting e-business, including: The WatchGuard LiveSecurity Broadcast Service, WatchGuard PolicyManager...

...LiveSecurity System can subscribe through PSINet,
GTE Internetworking, Verio, FASTNET and Interpath. The benefits of **outsourcing** security to a service provider include installation, policy configuration, 24x7 **security monitoring** by the service provider and automatic
distribution of the WatchGuard LiveSecurity updates.

Pricing and Availability...

26/3,K/24 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire

00321355 20000717199B3109 (USE FORMAT 7 FOR FULLTEXT)
DefendNet Solutions Expands Managed Security Offerings with Check Point Software's SiteManager-1 and Provider-1
Business Wire
Monday, July 17, 2000 09:03 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 525

...premier Internet security provider,"
said Vincent Giordano, president and CEO of DefendNet Solutions. "By incorporating **Check** Point's **security** technologies into our offerings, we will
be able to provide the enhanced services ISPs need...

...growing demand
for comprehensive, high-end Internet security solutions for a full range of enterprises."
" **Outsourcing** Internet security is becoming an increasingly attractive option
for many of today's e-businesses...
...Virtual Network
(SVN) architecture, SiteManager-1 combines a comprehensive, centralized management system at the provider **network operations center** with integrated
VPN/security capabilities on the customer premises. Provider-1 is Check Point's...

26/3,K/25 (Item 2 from file: 610)
DIALOG(R)File 610:Business Wire

(c) 2003 Business Wire. All rts. reserv.

00286609 20000523144B7413 (USE FORMAT 7 FOR FULLTEXT)
eGain Breaks New Ground in Delivering Next Generation of Hosting for Customer Service
Business Wire
Tuesday, May 23, 2000 16:46 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,022

...Service Level
Agreements. It enables unmatched implementation speed, guaranteed availability
and reliability, unparalleled protection with **multi** -level **security** , and **systems monitored** and operated by a highly experienced hosting team. Built
using a multi-level secure architecture...

...Based on
eGain's vast experience from hosting as well as feedback from their own **outsourcing** partners, the eGain Commerce 2000 platform easily enables remote
web administration, monitoring and tuning, and...

26/3,K/26 (Item 3 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2003 Business Wire. All rts. reserv.

00208901 20000306066B5176 (USE FORMAT 7 FOR FULLTEXT)
RIPTech Announces eSentry, First Application Service Provider Information Security Solution
Business Wire
Monday, March 6, 2000 11:33 EST
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,149

...also enables customers
to query and analyze their own data. Customers can either have RIPTech **analysts** manage **security** recommendations or have in-house IT staff take appropriate action.
RIPTech can either install eSentry...

...customer
site or integrate existing customer security products into the eSentry solution. eSentry includes comprehensive **outsourced** management of supported
security devices, including configuration and rule changes, as well as system
and...

26/3,K/27 (Item 4 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2003 Business Wire. All rts. reserv.

00199044 20000222053B4641 (USE FORMAT 7 FOR FULLTEXT)
Industry Leaders Support Check Point's New Cyber Attack Defense System;

Alteon, Anzen, Foundry, IBM, Tivoli, Intel, ISS, ODS, Veritas and WebTrends Announce Support
Business Wire
Tuesday, February 22, 2000 09:25 EST
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 970

TEXT:
...with a comprehensive security
infrastructure that gives them an added layer of protection against cyber **attacks** .

Check Point Software's Cyber Attack Defense System, announced on February 14,
includes **several** new **modules** and technologies, including the OPSEC Intrusion
Response Protocol. This new protocol automatically alerts third-party...
...said Asheem Chandna, vice president of business
development and product management, Check Point Software Technologies. "**Check**
Point's Cyber **Attack** Defense **System** , **integrated** with leading OPSEC products,
provides eBusinesses with the framework required to prevent cyber attacks."

26/3,K/28 (Item 5 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2003 Business Wire. All rts. reserv.

00109547 19990927270B1128 (USE FORMAT 7 FOR FULLTEXT)
ISS Extends ePatrol Managed Services -- Launches Scanning Service to Deliver Remote Security Assessment Solutions
Business Wire
Monday, September 27, 1999 08:19 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,166

...enable customers to put their security in the hands
of trusted experts who conduct 24x7 **security monitoring** and management
of their networks from a technically advanced **Network Operations Center**
(**NOC**). ISS is the only company to offer both an industry-leading
SAFEsuite(R) security management platform and Managed Security
Services. Together, these solutions deliver the software and **outsource**
options customers require for comprehensive information protection
across systems, databases, networks, services, and critical business...

26/3,K/29 (Item 6 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2003 Business Wire. All rts. reserv.

00053258 19990602153B1170 (USE FORMAT 7 FOR FULLTEXT)
MRT micro, Inc. Announces Camera Sales to Sandia National Laboratories
Business Wire
Wednesday, June 2, 1999 09:45 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE

WORD COUNT: 404

The MRT Observer/Eye cameras will be a component of the CMC's new remote **monitoring security** system. The cameras will be integrated as one of **many components** of their new **system** .

The CMC's mission is to assist political and technical experts from around the world...

26/3,K/30 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

13804042 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Cyber Security, Inc. Merges With the IS Consulting Group, Inc., Adding Consulting Services to its Managed Network Security Services
PR NEWSWIRE
November 15, 2000
JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 489

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... ID Intrusion Detection ISCG Information Solutions Consulting Group MSS Managed Security Services, Cyber Security's **outsourced** network security product. PKI Public Key Infrastructure **SOC Security Operations Center** , a 24x7x365 network monitoring and response facility. VPN Virtual Private Network, a network connection that...

26/3,K/31 (Item 2 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

12899113 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Cisco's Flagship Switching Platform Scales to Enhance E-Commerce Networks
BUSINESS WIRE
September 19, 2000
JOURNAL CODE: WBWE LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 1165

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... technology to scale both packet forwarding and flows per second. Cisco is also integrating an **Intrusion** Detection **System** (**IDS**) **module** into the Catalyst 6000 family for secure access to applications and corporate information. Along with...

... of service attack is detected. It also offers scalable traffic monitoring by load balancing across **multiple modules** and supports a full suite of over 300 attack signatures.
Pricing, Availability and Further Information

26/3,K/32 (Item 3 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

10502858 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Tendering goes on-line Government open to Net offers after launch of electronic system
NEIL ART
SOUTH CHINA MORNING POST, p1
April 11, 2000
JOURNAL CODE: FSCP LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 701

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... a third-party secure-hosting service. Anti-virus, firewall and intrusion detection software has been **integrated** into the **system** .
Application-level security was similar to that of the physical world, said Mr Yeung. The...

26/3,K/33 (Item 4 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

07456114 (USE FORMAT 7 OR 9 FOR FULLTEXT)
INTERNET SECURITY SYSTEMS: ISS extends ePatrol managed security services with scanning service
M2 PRESSWIRE
September 27, 1999
JOURNAL CODE: WMPR LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 385

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... 24x7 security monitoring and management of their networks from a technically advanced Network Operations Centre (**NOC**). ISS is the only company to offer both an industry-leading security management platform and Managed Security Services. Together, these solutions deliver the software and **outsource** options customers require for comprehensive information protection across systems, databases, networks, services, and critical business...

26/3,K/34 (Item 5 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

03220361 (USE FORMAT 7 OR 9 FOR FULLTEXT)
DMW's HostCHECK Provides the Power to Protect From the Inside Out! -- Announces Shipping of HostCHECK Version 2.0 for UNIX, Secure E-Business Solutions
BUSINESS WIRE
October 26, 1998
JOURNAL CODE: WBWE LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 900

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... the computer or files that, if tampered with, can be used for penetration purposes.
-- Assess -- **Several modules** perform a thorough security assessment on the host system. These include Directory Check, Integrity Check...

26/3,K/42 (Item 2 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

087868
Hands-off Management
Management service providers let you offload operational tasks yet retain control of your network, but be careful about which MSP you choose.
Byline: By Elisabeth Horwitt
Journal: Network World Page Number: 58
Publication Date: October 09, 2000
Word Count: 1950 Line Count: 179

Text:
...of systems engineering at Homestead.com, has good reason to be leery of systems management **outsourcing** . His Web-hosting company tried such an arrangement with its ISPs, and suffered serious service...

... provide 24-7 support for its primary Web site. Alerts go first to SiteRock's **network operations center** , where technicians handle low-level problems and escalate everything else to Homestead. com's staff ...

... is one of a growing number of businesses that find the MSP model attractive. Unlike **outsourcing** companies that take full responsibility for systems management, MSPs essentially let customers have it their...

...says John McConnell, president of McConnell Associates in Boulder, Colo. "It's the advantage of **outsourcing** without the risks of surrendering everything." MSPs basically appeared out of nowhere early this year...

... an in-house IT manager. Then there are the MSP setups that border on full **outsourcing** . For example, SiteLite not only handles network monitoring, but also proactive maintenance and administration, says...MSP (see "shopping advice," page 59). Furthermore, early adopters say an MSP relationship, like any **outsourcing** arrangement, needs considerable up-front planning and established policies and procedures in order to work ...

... vulnerable because the Web is the lifeline that links customer systems to the MSP's **network operations center** . "We can't guarantee that someone won't put a backhoe through the wire," TriActive...

... management and data storage while sending key data over the Web to the MSP's **network operations center** . If the link goes down, the server provides a management database, alerting, discovery, reporting, **security** scanning and performance **monitoring** at the site for up to seven days, Igoe says. That's fine if the...

26/3,K/43 (Item 3 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

087475
Cisco boosts core LAN switch features
Catalyst 6000 gets 256G bit/sec switch fabric, management and Gigabit Ethernet modules.
Byline: JIM DUFFY

Journal: Network World Page Number: 27
Publication Date: September 25, 2000
Word Count: 621 Line Count: 62

Text:
... CEF) technology to improve packet and flow performance. Cisco is also integrating a so-called **Intrusion** Detection **System** (**IDS**) **module** into the Catalyst 6000 family for secure access to applications and corporate information. The services...

... TCP session termination and access control list configuration in the event a denial-of-service **attack** is **detected** . It also provides scalable traffic monitoring by load balancing across **multiple modules** , Cisco says. The switching fabric module costs $7,495, the Supervisor 2 module $34,995...

26/3,K/44 (Item 4 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

083486
10 companies to watch
From CLECs to application-aware switch vendors, these start-ups warrant your attention.
Byline: BETH SCHULTZ
Journal: Network World Page Number: 95
Publication Date: April 24, 2000
Word Count: 2201 Line Count: 210

Text:
... new start-up in February.As is the fashion these days, Loudcloud has entered the **outsourcing** realm. It does so with Web site automation technology called Opsware and a services package s really all that needs to be said about why we've included an **intrusion - detection** company on our watch list. But we can say plenty more about why Network ICE...

... detects uninvited visitors, it reports the intrusion to the ICEcap management module. In turn, ICEcap **analyzes** the **intrusion** information from the agents and uses it to spot widescale attacks on a network. Intel ...
... afoot in the systems management industry: Fledgling and established vendors alike are heavily pushing automated, **integrated** management **systems** for networks, systems and applications. Start-up RiverSoft is in the thick of it. In...

... management applications.SilverBack gives customers a homegrown, Linux-based device that runs off-the-shelf **monitoring** , reporting and **security** tools and customized application software. The box sits on a critical path, say off the...SilverBack unveiled InfoCare in late February. It offers network alerts, asset inventory, network infrastructure performance **monitoring** and **security** scanning applications. Later iterations will add **intrusion detection** , root cause **analysis** , application monitoring and network virus scanning. Top Layer NetworksOnce known as BlazeNet and focused on...

26/3,K/45 (Item 5 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

076165
BorderWare: Response to firewall RFP
Journal: Network World
Publication Date: July 19, 1999
Word Count: 1516 Line Count: 150

Text:
... standby system. The configuration of this backup system should be kept in step with the **primary system** . This can be done locally by following a very simple procedure on the Firewall console... purchased at an additional cost. Alarms and Log AnalysisThe BorderWare Firewall Server includes facilities to **monitor** attempted **attacks** and to raise alarms in real-time. No **additional components** are needed.The BorderWare Firewall Server produces extensive logs, a third party log analysis tool...

26/3,K/46 (Item 6 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

074919
Tivoli seeks interoperability for mgmt. tools
Byline: JEFF CARUSO
Journal: Network World
Publication Date: May 24, 1999
Word Count: 783 Line Count: 73

Text:
... to happen" because all the policy servers that have been announced are aimed at the **network operations center** , Cole says. The people in the **network operations center** are not the people who should make decisions about which applications and departments get top...

... to set policies through Tivoli software and pass them on to various policy servers in **network operations centers** . "We will allow you to gain control over what is going to be chaos in...

... also be getting a new interface that can launch Web-based management interfaces embedded in **many** network **devices** today.This feature appeals to Bengt-Olof Bloom, a network engineer with the Swedish bank...
... has a separate management system for ATM and that he would like to see that **system integrated** with NetView.On the systems management side, Tivoli is preparing Tivoli Manager on OS/390...

... framework to the OS/390 platform so that network managers can run software distribution, inventory, **security** and systems **monitoring** from there. The Manager software will collect information about applications on the mainframe to determine...

26/3,K/47 (Item 7 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

074608
Response to RFP: Radguard
Journal: Network World
Publication Date: May 10, 1999
Word Count: 954 Line Count: 97

Text:
... Powell to purchase a managed service with one of Radguard's partners, whereby installation, management, **security monitoring** , etc. will be **outsourced** . This will entail a different pricing structure, to be determined with the said partner.Network...

... least remote access, it might choose to use the connection for other purposes. The cIPro- **System** 's **components** can provide firewall functionality to allow Powell to use this connection securely.Redundancy. The cIPro...

26/3,K/48 (Item 8 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

074565
VPN RFP - Radguard
Journal: Network World
Publication Date: May 10, 1999
Word Count: 990 Line Count: 98

Text:
... Powell to purchase a managed service with one of Radguard's partners, whereby installation, management, **security monitoring** , etc. will be **outsourced** . This will entail a different pricing structure, to be determined with the said partner.- Network...

... least remote access, it might choose to use the connection for other purposes. The cIPro- **System** 's **components** can provide firewall functionality to allow Powell to use this connection securely.- Redundancy. The cIPro...

26/3,K/49 (Item 9 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

070585
Executive Briefing
r
Byline: n/a
Journal: Computerworld Page Number: 2
Publication Date: November 23, 1998
Word Count: 457 Line Count: 41

Text:
... volume requirements, analysts said. It's probably too late for massive upgrades, but analysts recommend **checking** into **subsystems** and **security** , load balancing and **outsourcing** . Page 4
pPurchasing and finance managers find tremendous payback in online buying systems, but getting...

26/3,K/50 (Item 10 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

053697

Inside Lines
Inside Lines
Inside Lines
Byline: Inside Lines
Journal: Computerworld Page Number: 94
Publication Date: August 05, 1996
Word Count: 533 Line Count: 50

Text:
... add Internet security to the wide-area network and systems management services provided by its **network operations center** in Austin, Texas. Organizations can then **outsource** such tasks as **security assessment** , firewall setup and **monitoring** of an **intrusion detection** and response system.
A fight may be brewing
In an about-face, SAP AG which...

26/3,K/51 (Item 11 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

048253
RMON holds service promise
Byline: Joanie Wexler
Journal: Network World Page Number: 24
Publication Date: November 20, 1995
Word Count: 334 Line Count: 32

Text:
Innovative developments with Remote Monitoring (RMON) technology will be a boon to **outsourced** monitoring services once a few problems get solved. RMON is the network management standard for...

...Shipping volumes of monitoring data across a customer's net to the third party's **network operations center** can clog the user's network, pointed out John McConnell, president of McConnell Consulting, Inc...

... flag for users is that they must be able to retain some control over network **security** . RMON **probes** could be used to pick up user passwords, McConnell pointed out. To ease users' minds...

```
File   9:Business & Industry(R) Jul/1994-2003/May 05
         (c) 2003 Resp. DB Svcs.
File  16:Gale Group PROMT(R) 1990-2003/May 05
         (c) 2003 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2003/May 02
         (c) 2003 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2003/May 05
         (c)2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2003/May 05
         (c) 2003 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2003/May 05
         (c) 2003 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2003/May 05
         (c) 2003 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2003/May 05
         (c) 2003 The Gale Group
? ds

Set     Items   Description
S1    2127105   INTRUS????? ? OR INTRUD???? ? OR ATTACK???? ? OR PSEUDOATT-
             ACK? OR VULNERAB? OR HACK???? ? OR CRACK???? ? OR MALICIOUS OR
              UNAUTHORIZ? OR UNAUTHORIS? OR INFILTRAT? OR THREAT?
S2    1993511   SECURITY
S3      36458   IDS
S4     554062   PENETRAT? OR BREACH?
S5     131435   S1:S4(3N)(TRACK? OR DETECT? OR MONITOR? OR DISCERN? OR GAU-
             G??? ? OR EXPOS???? ? OR CHECK??? ? OR CHEQU??? ? OR DIAGNOS?-
             ?? ?)
S6      74731   S1:S4(3N)(SELFTEST? OR SELFDIAGNOS? OR DX OR PROBE? ? OR P-
             ROBING? OR ANALYS? OR ANALYZ? OR ANALYT? OR ASSESS????? ? OR -
             BIST)
S7      41820   S1:S4(3N)(EVALUAT? OR SENS?R? ? OR SENSING OR SENSE? ? OR -
             SCREEN?)
S8      37318   NOC OR NETWORK? ?(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CEN-
             TER? ? OR CENTRE? ?)
S9      63504   SOC OR SECURITY(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CENTE-
             R? ? OR CENTRE? ?)
S10  10626014   SYSTEM? ?
S11    499698   S10(3N)(INTEGRATED OR MASTER OR PRINCIPAL OR MAIN OR PARENT
              OR HIERARCH? OR TOPOLOG? OR PRIMARY)
S12    163746   SUBSYSTEM? OR SUB()SYSTEM?
S13      7778   S10(3N)(MULTI()(LAYER? OR LEVEL? OR TIER? OR STACK? OR BRA-
             NCH?) OR MULTILAYER? OR MULTILEVEL? OR MULTITIER? OR MULTISTA-
             CK? OR MULTIBRANCH?)
S14      2856   S10(3N)(MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIP-
             LE OR MULTIPLICIT? OR MULTITUD? OR ADDITIONAL)(1W)(LAYER? OR -
             LEVEL? OR TIER? OR STACK? OR BRANCH?)
S15    360379   FIREWALL? OR FIRE()WALL? ? OR ROUTER? ? OR S3
S16       249   MULTIDEVICE?
S17     61487   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
             ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
             VARIOUS OR VARIETY)(1W)DEVICE?
S18    415173   OUTSOURC? OR OUT()SOURC??? ?
S19       990   S5:S7(S)S8:S9
S20      3248   S5:S7(S)(S11:S14 OR SUBCOMPONENT? OR SUBMODULE? OR S10(3N)-
            (COMPONENT? OR MODULE?))
S21     86643   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
             ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
             VARIOUS OR VARIETY)(1W)(COMPONENT? OR MODULE?)
```

S22	512	S20(S)(S15:S18 OR S21)
S23	63	S20(S)(S16:S18 OR S21)
S24	16	S23/2001:2003
S25	47	S23 NOT S24
S26	29	RD (unique items)

26/3,K/6 (Item 6 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06329304 Supplier Number: 54597528 (USE FORMAT 7 FOR FULLTEXT)
WatchGuard Showcases LiveSecurity Broadcast Service at N+I.
PR Newswire, p7012
May 11, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 618

... working with systems security since 1984.
The WatchGuard LiveSecurity Family of Solutions
The WatchGuard LiveSecurity **System** delivers the **components** designed to protect companies conducting e-business, including: The WatchGuard LiveSecurity Broadcast Service, WatchGuard PolicyManager...

...LiveSecurity System can subscribe through PSINet, GTE Internetworking, Verio, FASTNET and Interpath. The benefits of **outsourcing** security to a service provider include installation, policy configuration, 24x7 **security monitoring** by the service provider and automatic distribution of the WatchGuard LiveSecurity updates.
Pricing and Availability...

26/3,K/7 (Item 7 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05581539 Supplier Number: 48450031 (USE FORMAT 7 FOR FULLTEXT)
REPEATING/ DMW Introduces HostCHECK for UNIX Advanced Security Tool Set.
Business Wire, p04280228
April 28, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 978

... security configuration of the computer or files that, if tampered with, can be used for **penetration** purposes.
o **Assess - Several modules** perform a thorough security assessment on the host system. These include Directory Check, Integrity Check...

26/3,K/19 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10986737 SUPPLIER NUMBER: 54483407 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Greater integration key to active firewalls.(Feature Report: Security)
Malezis, Gus
Computer Dealer News, 15, 5, 26(1)
Feb 15, 1999
ISSN: 1184-2369 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 658 LINE COUNT: 00061

... and systems - as well as specific areas within the intranet such as finance. The resulting **multi - layered** security **system** is comprised of **several** security **devices** , including multiple firewalls, VPNs, **Intrusion Detection** Systems (**IDS**) and Authorization and Authentication systems, as well as virus protection and data encryption software.
The...

26/3,K/28 (Item 3 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

02992159 Supplier Number: 46103588 (USE FORMAT 7 FOR FULLTEXT)
IBM: IBM announces SecureWay line of Internet security products and services
M2 Presswire, pN/A
Jan 30, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 489

... software
* distributed security management
* directory and security services for LAN servers.
Security features are also **integrated** into IBM operating **systems** , network and database programs and Lotus Notes which has embedded public key cryptography. offerings for...

...T Security consulting practice Emergency Response Service; ethical hacking, backed by IBM Research's Global **Security Analysis** Lab; anti-virus; **security** implementation and **outsourcing** services; and turnkey firewall installation services.
"IBM has had a long history in developing security...

```
File   2:INSPEC 1969-2003/Apr W4
         (c) 2003 Institution of Electrical Engineers
File   6:NTIS 1964-2003/May W1
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2003/Apr W3
         (c) 2003 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2003/Apr W4
         (c) 2003 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2003/Apr
         (c) 2003 ProQuest Info&Learning
File  65:Inside Conferences 1993-2003/Apr W4
         (c) 2003 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2003/Apr W4
         (c)2003 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2003/Apr W3
         (c) 2003 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Mar
         (c) 2003 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/May 02
         (c) 2003 The Gale Group
File 144:Pascal 1973-2003/Apr W4
         (c) 2003 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2003/Apr 04
         (c) Information Today, Inc
File 233:Internet & Personal Comp. Abs. 1981-2003/Apr
         (c) 2003 Info. Today Inc.
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2003/May 05
         (c) 2003 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
? ds

Set     Items   Description
S1    1556278   INTRUS????? ? OR INTRUD???? ? OR ATTACK???? ? OR PSEUDOATT-
              ACK? OR VULNERAB? OR HACK???? ? OR CRACK???? ? OR MALICIOUS OR
               UNAUTHORIZ? OR UNAUTHORIS? OR INFILTRAT? OR THREAT?
S2     418778   SECURITY  (January 1993)
S3       6949   IDS
S4     318838   PENETRAT? OR BREACH?
S5      51786   S1:S4(3N)(TRACK? OR DETECT? OR MONITOR? OR DISCERN? OR GAU-
              G??? ? OR EXPOS???? ? OR CHECK??? ? OR CHEQU??? ? OR DIAGNOS?-
              ?? ?)
S6      90016   S1:S4(3N)(SELFTEST? OR SELFDIAGNOS? OR DX OR PROBE? ? OR P-
              ROBING? OR ANALYS? OR ANALYZ? OR ANALYT? OR ASSESS????? ? OR -
              BIST)
S7      28016   S1:S4(3N)(EVALUAT? OR SENS?R? ? OR SENSING OR SENSE? ? OR -
              SCREEN?)
S8       2481   NOC OR NETWORK? ?(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CEN-
              TER? ? OR CENTRE? ?)
S9      33347   SOC OR SECURITY(1W)(OPERATION? ? OR OPN OR OPNS)(1W)(CENTE-
              R? ? OR CENTRE? ?)
S10  13369810   SYSTEM? ?
S11    267046   S10(3N)(INTEGRATED OR MASTER OR PRINCIPAL OR MAIN OR PARENT
               OR HIERARCH? OR TOPOLOG? OR PRIMARY)
S12    108722   SUBSYSTEM? OR SUB()SYSTEM?
S13     22735   S10(3N)(MULTI()(LAYER? OR LEVEL? OR TIER? OR STACK? OR BRA-
              NCH?) OR MULTILAYER? OR MULTILEVEL? OR MULTITIER? OR MULTISTA-
              CK? OR MULTIBRANCH?)
S14      2101   S10(3N)(MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIP-
```

```
          LE OR MULTIPLICIT? OR MULTITUD? OR ADDITIONAL)(1W)(LAYER? OR -
          LEVEL? OR TIER? OR STACK? OR BRANCH?)
S15     42655   FIREWALL? OR FIRE()WALL? ? OR ROUTER? ? OR S3
S16       112   MULTIDEVICE?
S17     20760   (MANY OR SEVERAL OR PLURALITY OR NUMEROUS OR MULTIPLE OR M-
          ULTIPLICIT? OR MULTITUD? OR ADDITIONAL OR MULTI OR NUMBER OR -
          VARIOUS OR VARIETY)(1W)DEVICE?
S18     24923   OUTSOURC? OR OUT()SOURC??? ?
S19        63   S5:S7 AND S8:S9
S20      1955   S5:S7 AND S11:S14
S21        63   S19:S20 AND S15:S18
S22        25   S21/2001:2003
S23        38   S21 NOT S22
S24        28   RD (unique items)
```

24/7/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6622433 INSPEC Abstract Number: B2000-07-6150M-080, C2000-07-5640-072
Title: A design of scalable SNMP agent for managing heterogeneous security systems
Author(s): Lee, D.Y.; Kim, D.S.; Pang, K.H.; Kim, H.S.; Chung, T.M.
Author Affiliation: Dept. of Electr. & Comput. Eng., Sungkyunkwan Univ., Suwon-City, South Korea
Conference Title: NOMS 2000. 2000 IEEE/IFIP Network Operations and Management Symposium `The Networked Planet: Management Beyond 2000' (Cat. No.00CB37074) p.983-4
Editor(s): Hong, J.W.; Weihmayer, R.
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2000 Country of Publication: USA xxvii+1022 pp.
ISBN: 0 7803 5928 3 Material Identity Number: XX-1999-03415
Conference Title: Proceedings of Network Operations and Management Symposium
Conference Date: 10-14 April 2000 Conference Location: Honolulu, HI, USA
Medium: Alos available on CD-ROM in PDF format
Language: English Document Type: Conference Paper (PA)
Treatment: Applications (A)
Abstract: This paper presents a Web based **integrated** security management **system** (WISMS) which has been developed to **monitor** and control heterogeneous **security** systems and the detailed design of **firewall** agents. The agents perform the control requests from the security manager, maintain the **firewall** MIB (management information base), and report the monitored status of the **firewall** . (0 Refs)
Subfile: B C

24/7/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

6497997 INSPEC Abstract Number: B2000-03-6150M-060, C2000-03-5640-048
Title: Intrusion detection **for link state routing protocol through integrated network management**
Author(s): Feiyi Wang; Gong, F.; Wu, F.S.; Narayan, R.
Author Affiliation: Adv. Networking Res. Group, MCNC, Research Triangle Park, NC, USA
Conference Title: Proceedings Eight International Conference on Computer Communications and Networks (Cat. No.99EX370) p.634-9
Editor(s): Dixit, S.; Somani, A.; Park, E.
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 1999 Country of Publication: USA xix+661 pp.
ISBN: 0 7803 5794 9 Material Identity Number: XX-1999-03070
U.S. Copyright Clearance Center Code: 0 7803 5794 9/99/$10.00
Conference Title: Proceedings of IC3N'99: Eighth International Conference on Computer Communications and Networks
Conference Sponsor: Army Res. Lab.; Nokia; IEEE Commun. Soc
Conference Date: 11-13 Oct. 1999 Conference Location: Boston, MA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Experimental (X)
Abstract: The JiNao **IDS** project focuses on **detecting intrusions**, especially insider **attacks** against link state routing protocols such as OSPF. One important feature of the JiNao **system** is its **integrated** network management (INM) capability. Through SNMP and distributed programming interface (DPI), we can manage and control distributed JiNao **IDS** remotely, interoperate with other JiNao systems to do correlation analysis, and utilize both private MIB and OSPF MIB as a complementary way of doing **intrusion detection**. This paper describes the design and implementation of JiNao's INM architecture. Three OSPF insider attacks (maxseq, maxage, and seq++) have been developed to evaluate its effectiveness and detection capability. (17 Refs)
Subfile: B C

24/7/6 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

5544770 INSPEC Abstract Number: B9705-6210C-015, C9705-6130S-026
Title: Intrusion detection : **a survey**
Author(s): Esmaili, M.; Safavi-Naini, R.; Pieprzyk, J.
Author Affiliation: Center for Comput. Security Res., Wollongong Univ., NSW, Australia
Conference Title: Information Highways for a Smaller World and Better Living. Proceedings of ICCC'95. (12th International Conference on Computer Communication) p.409-14
Editor(s): Chung, S.J.
Publisher: IOS Press, Amsterdam, Netherlands
Publication Date: 1995 Country of Publication: Netherlands xxxxii+862 pp.
Material Identity Number: XX95-01319
Conference Title: ICCC'95 - International Conference on Computer Communications
Conference Sponsor: ICCC-Int. Council for Comput. Commun.; Minstr. Inf. & Commun., Republic of Korea
Conference Date: 21-24 Aug. 1995 Conference Location: Seoul, South Korea
Language: English Document Type: Conference Paper (PA)
Treatment: General, Review (G)
Abstract: Advances in computer and communication technologies have resulted in highly **integrated** distributed **systems** that allow users to access information and resources from all over the globe. This interconnectivity adds new dimensions to the long-standing problem of providing security in a computer system by introducing many more possible attacking points. Rapid increase in the number of reported intrusions, break-ins and computer thefts results in an ever-increasing need for applying effective computer security measures. The number of recently developed, or under-development, systems and tools that can be used for detection of abuse of computer systems is growing. We present a comparative review of the state-of-the-art **intrusion detection** systems (**IDS**) and techniques and underline the strength and limitations of each. We will also point out directions for future development and research. (21 Refs)
Subfile: B C

24/7/12 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

2202129 NTIS Accession Number: ADA391492/XAB
Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems
Mell, P. ; McLarnon, M.
National Inst. of Standards and Technology, Gaithersburg, MD.
Corp. Source Codes: 092732000; 419591
10 Aug 1999 9p
Languages: English
Journal Announcement: USGRDR0121
Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)605-6900; and email at orders@ntis.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A02/MF A01
Country of Publication: United States
Distributed **intrusion detection** systems are especially **vulnerable** to attacks because the components reside at a static location and are connected together into a hierarchical structure. An attacker can disable such a system by taking out a node high in the hierarchy, thus amputating a portion of the distributed system. One solution to this problem is to cast the internal nodes in the **system hierarchy** as mobile agents. These mobile agents randomly move around the network such that an attacker can not locate their position. If an attacker takes out a mobile agent platform, the remaining agents estimate the location of the attacker and automatically avoid those networks. Killed agents are resurrected by a group of backups that retain all or partial state information. We are implementing this technology as an API such that existing **intrusion detection** systems can wrap their components as mobile agents in order to gain a type of 'attack resistance'.

24/7/18 (Item 7 from file: 6)
DIALOG(R)File 6:NTIS

1680202 NTIS Accession Number: DE92016335
Wireless data communications
Christiansen, M. L. ; Harrington, J. J. ; Outwater, M.
Sandia National Labs., Albuquerque, NM.
Corp. Source Codes: 068123000; 9511100
Sponsor: Department of Energy, Washington, DC.
Report No.: SAND-92-1313C; CONF-9206197-1
1992 9p
Languages: English Document Type: Conference proceeding
Journal Announcement: GRAI9224; ERA9251
American Defense Preparedness Association (ADPA) government-industry symposium on security technology, Williamsburg, VA (United States), 1-4 Jun 1992. Sponsored by Department of Energy, Washington, DC.
U.S. Sales Only. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A02/MF A01
Country of Publication: United States
Contract No.: AC04-76DP00789
A primary function of an **Intrusion Detection** System (**IDS**) is to convey system status from remote sensing points to manned collection stations. The bulk of these systems rely on communications channels that the implemented with physical connections composed of either metallic wire or glass fiber. While these channels provide connectivity for the **IDS** , a definite liability resulting from the physical nature of the channels is encountered. This liability manifests itself primarily during system installation when significant costs arising from labor are encountered. The time required to install physical channels is also a liability which may prohibit its use in semipermanent or rapidly deployable applications. To address these limitations, the Dispersed **Integrated** Security **System** (DISS) Program has adopted a philosophy of wireless communications links to be used where appropriate in conjunction with standard wire- and fiber-based systems. When low-cost, rapidly deployable systems are required, Radio Frequency (RF) links are offered. DISS RF links are well suited for applications ranging from tactical to semipermanent sites. Other wireless links being considered for special DISS applications may take advantage of narrow-beam microwave and infrared technologies. Alongside these wireless devices, conventional wire and fiber systems may also be used to fulfill critical security requirements. This paper lists the system requirements that DISS intends to meet and describes the communications equipment that comprises DISS from a hardware and user perspective. System capabilities are highlighted in the context of operational scenarios, and DISS communications is summarized in the final section.

24/7/19 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05745459 E.I. No: EIP00125457389
Title: Adaptation techniques for intrusion detection **and** intrusion **response systems**
Author: Ragsdale, Daniel J.; Carver, Curtis A. Jr.; Humphries, Jeffrey W. ; Pooch, Udo W.
Corporate Source: United States Military Acad, USA

Conference Title: 2000 IEEE International Conference on Systems, Man and Cybernetics
Conference Location: Nashville, TN, USA Conference Date: 20001008-20001011
Sponsor: IEEE
E.I. Conference No.: 57755
Source: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics v 4 2000. IEEE, Piscataway, NJ, USA,00CB37166. p 2344-2349
Publication Year: 2000
CODEN: PICYE3 ISSN: 0884-3627
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0102W2
Abstract: This paper examines techniques for providing adaptation in **intrusion detection** and **intrusion** response systems. As attacks on computer systems are becoming increasingly numerous and sophisticated, there is a growing need for **intrusion detection** and response systems to dynamically adapt to better **detect** and respond to **attacks** . The Adaptive Hierarchical Agent-based **Intrusion Detection** System (AHA **IDS**) provides **detection** adaptation by adjusting the amount of system resources devoted to the task of **detecting intrusive** activities. This is accomplished by dynamically invoking new combinations of lower level detection agents in response to changing circumstances and by adjusting the confidence associated with these lower-level agents. The Adaptive Agent-based Intrusion Response System (AAIRS) provides response adaptation by weighting those responses that have been successful in the past over those techniques that have not been as successful. As a result, the more successful responses are used more often than the less successful techniques. It also adapts responses based on the system's belief that **intrusion detection** reports are valid. Intuitively, adaptive detection and response systems will provide more robust protection than static, non-adaptive systems. (Author abstract) 27 Refs.

24/7/20 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05733375 E.I. No: EIP00125435698
Title: Intrusion detection **in wireless ad-hoc networks**
Author: Zhang, Yongguang; Lee, Wenke
Corporate Source: HRL Lab, Malibu, CA, USA
Conference Title: 6th Annual International Conference on Mobile Computing and Networking (MOBICOM 2000)
Conference Location: Boston, MA, USA Conference Date: 20000806-20000811
Sponsor: ACM SIGMOBILE
E.I. Conference No.: 57709
Source: Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM 2000. ACM, New York, NY, USA. p 275-283
Publication Year: 2000
CODEN: 002378
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0101W4
Abstract: As the recent denial-of-service attacks on several major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the **intrusion detection** techniques

developed on a fixed wired network are not applicable in this new environment. How to do it differently and effectively is a challenging research problem. In this paper, we first examine the vulnerabilities of a wireless ad-hoc network, the reason why we need **intrusion detection** , and the reason why the current methods cannot be applied directly. We then describe the new **intrusion detection** and response mechanisms that we are developing for wireless ad-hoc networks. (Author abstract) 17 Refs.

24/7/22 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04566298 E.I. No: EIP96113428749
Title: Proceedings of the 1996 30th IEEE Annual International Carnahan Conference on Security Technology
Author: Sanson, L.D. (Ed.)
Conference Title: Proceedings of the 1996 30th IEEE Annual International Carnahan Conference on Security Technology
Conference Location: Lexington, KY, USA Conference Date: 19961002-19961004
Sponsor: IEEE
E.I. Conference No.: 45647
Source: IEEE Annual International Carnahan Conference on Security Technology, Proceedings 1996. IEEE, Piscataway, NJ, USA,96CH35975. 256p
Publication Year: 1996
CODEN: 85QRAQ
Language: English
Document Type: CP; (Conference Proceedings) Treatment: A; (Applications); G; (General Review); T; (Theoretical)
Journal Announcement: 9701W3
Abstract: The proceedings contains 40 papers from the 1996 IEEE International Carnahan Conference on Security Technology. Topics discussed include: security systems, closed circuit television (CCTV) systems, image processing, sensor data fusion, infrared detectors, synergistic radar systems, millimeter wave holography, obstacle avoidance, personnel tracking systems, digital mobile communication systems, interconnection networks, data security, cryptography, fingerprint identification, facial identification, network protocols, access control, intelligent control, annunciator systems, **security** risk assessment and **analysis** , **intruder detection** systems (**IDS**), police duty scheduling and earthquake prediction systems.

24/7/26 (Item 1 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

01450141 20000905210
Intrusion Detection **in grossen Netzen: Mehr Sicherheit durch Verteilung?**
Ockl, AB
RWTH Aachen, D
Online 2000, 23. Europaeische Congressmesse fuer technische Kommunikation, Congress IV: Telekommunikations-Sicherheit & Security Management, Duesseldorf, D, 31.01.-03.02.20002000
Document type: Conference paper Language: German
Record type: Abstract
ISBN: 3-89077-209-9

ABSTRACT:
Viele Firmen haben nahezu alle wichtigen Daten in ihrem Netzwerk abgelegt, so dass der Verlust oder die Veroeffentlichung dieser Daten im schlimmsten Fall die Existenz des Unternehmens bedrohen kann. Und trotzdem wird die Sicherheit vielerorts vernachlaessigt bzw. unterschaetzt, da Sicherheit hohe Kosten ohne sichtbaren Gewinn verursacht. **Intrusion Detection** Systeme erkennen interne und externe Angriffe innerhalb eines Netzwerkes. Da moderne **Intrusion Detection** Systeme dabei als verteilte Systeme agieren, nennt man sie auch verteilte **Intrusion Detection** Systeme. Im Gegensatz zu **Firewallsysteme** installieren die gaengigen verteilten **Intrusion Detection** Systeme dabei zur Datensammlung innerhalb des Netzwerkes Sensoren, die moeglichst viele Ueberwachungsdaten sammeln. Anforderungen an ein lntrusion Detection System lassen sich aus zwei Perspektiven betrachten. Zum einen werden Anforderungen an die Dienste gestellt, die es zum Schutz des zu ueberwachenden Systems bereitstellt. Als ueberwachendes System ist das **Intrusion Detection** System jedoch selbst auch Angriffsziel und muss deshalb strengen Schutzanforderungen genuegen. Ausserdem sollte das **Intrusion Detection** System nach einem Angriff bzw. Systemversagen wieder in einen korrekten Ursprungszustand versetzbar sein, um die Ueberwachung fortzusetzen (Fehlertoleranz des **Intrusion Detection** Systems). Ausserdem ist zu beachten, dass keine Software fehlerfrei ist, also auch das lntrusion Detection System nicht. Da Fehler von Angreifern als Angriffspunkte benutzt werden, kann der komplette Schutz durch das lntrusion Detection System nicht gewaehrleistet werden. Das sollte in der Architektur des **Intrusion Detection** Systems beruecksichtigt sein. Es muss also eingeplant werden, dass Angriffe erfolgreich sein koennen und einzelne Teilkomponenten ausfallen bzw. uebernommen werden. Das System sollte den Ausfall von Teilkomponenten bzw. **Subsystemen** verkraften koennen (Ausfallsicherheit), so dass das Restsystem in seinem korrekten Ablauf so wenig wie moeglich gestoert wird. Das wird je eher erreicht, je weniger das System zentral koordiniert wird und je redundanter bzw. ersetzbarer die Komponenten sind.